National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 31 Mar 2023 Vol. 10 No. 06

Table of Content

Vendor	Product	Page Number
Cisco	asr_920-12cz-d	936
	asr_920-12cz-d_r	937
	asr_920-12sz-im	939
	asr_920-12sz-im_r	940
	asr_920-24sz-im	942
	asr_920-24sz-im_r	943
	asr_920-24sz-m	944
	asr_920-24sz-m_r	946
	asr_920-24tz-m	947
	asr_920-24tz-m_r	948
	asr_920-4sz-a	950
	asr_920-4sz-a_r	951
	asr_920-4sz-d	952
	asr_920-4sz-d_r	954
	asr_920u-12sz-im	955
	asr_9901	957
	asr_9902	958
	asr_9903	959
	asr_9904	961
	asr_9906	962
	asr_9910	963
	asr_9912	965
	asr_9920	966
	asr_9922	968
	catalyst_3650	969
	catalyst_3650-12x48fd-e	970
	catalyst_3650-12x48fd-l	971
	catalyst_3650-12x48fd-s	972
	catalyst_3650-12x48uq	973
	catalyst_3650-12x48uq-e	974
	catalyst_3650-12x48uq-l	975
	catalyst_3650-12x48uq-s	975

Vendor	Product	Page Number
Cisco	catalyst_3650-12x48ur	977
	catalyst_3650-12x48ur-e	977
	catalyst_3650-12x48ur-l	978
	catalyst_3650-12x48ur-s	979
	catalyst_3650-12x48uz	981
	catalyst_3650-12x48uz-e	981
	catalyst_3650-12x48uz-l	982
	catalyst_3650-12x48uz-s	983
	catalyst_3650-24pd	985
	catalyst_3650-24pd-e	985
	catalyst_3650-24pd-l	986
	catalyst_3650-24pd-s	987
	catalyst_3650-24pdm	989
	catalyst_3650-24pdm-e	989
	catalyst_3650-24pdm-l	990
	catalyst_3650-24pdm-s	991
	catalyst_3650-24ps-e	992
	catalyst_3650-24ps-l	993
	catalyst_3650-24ps-s	994
	catalyst_3650-24td-e	995
	catalyst_3650-24td-l	996
	catalyst_3650-24td-s	997
	catalyst_3650-24ts-e	998
	catalyst_3650-24ts-l	999
	catalyst_3650-24ts-s	1000
	catalyst_3650-48fd-e	1001
	catalyst_3650-48fd-l	1002
	catalyst_3650-48fd-s	1003
	catalyst_3650-48fq	1005
	catalyst_3650-48fq-e	1005
	catalyst_3650-48fq-l	1006
	catalyst_3650-48fq-s	1007

Vendor	Product	Page Number
Cisco	catalyst_3650-48fqm	1009
	catalyst_3650-48fqm-e	1009
	catalyst_3650-48fqm-l	1010
	catalyst_3650-48fqm-s	1011
	catalyst_3650-48fs-e	1012
	catalyst_3650-48fs-l	1013
	catalyst_3650-48fs-s	1014
	catalyst_3650-48pd-e	1015
	catalyst_3650-48pd-l	1016
	catalyst_3650-48pd-s	1017
	catalyst_3650-48pq-e	1018
	catalyst_3650-48pq-l	1019
	catalyst_3650-48pq-s	1020
	catalyst_3650-48ps-e	1021
	catalyst_3650-48ps-l	1022
	catalyst_3650-48ps-s	1023
	catalyst_3650-48td-e	1024
	catalyst_3650-48td-l	1025
	catalyst_3650-48td-s	1026
	catalyst_3650-48tq-e	1027
	catalyst_3650-48tq-l	1028
	catalyst_3650-48tq-s	1029
	catalyst_3650-48ts-e	1030
	catalyst_3650-48ts-l	1031
	catalyst_3650-48ts-s	1032
	catalyst_3650-8x24pd-e	1033
	catalyst_3650-8x24pd-l	1034
	catalyst_3650-8x24pd-s	1035
	catalyst_3650-8x24uq	1037
	catalyst_3650-8x24uq-e	1037
	catalyst_3650-8x24uq-l	1038
	catalyst_3650-8x24uq-s	1039

Vendor	Product	Page Number
Cisco	catalyst_3850-48f-s	1112
	catalyst_3850-48p-e	1115
	catalyst_3850-48p-l	1117
	catalyst_3850-48p-s	1119
	catalyst_3850-48pw-s	1121
	catalyst_3850-48t-e	1124
	catalyst_3850-48t-l	1126
	catalyst_3850-48t-s	1128
	catalyst_3850-48u	1130
	catalyst_3850-48u-e	1133
	catalyst_3850-48u-l	1135
	catalyst_3850-48u-s	1137
	catalyst_3850-48xs	1139
	catalyst_3850-48xs-e	1142
	catalyst_3850-48xs-f-e	1144
	catalyst_3850-48xs-f-s	1146
	catalyst_3850-48xs-s	1148
	catalyst_3850-nm-2-40g	1151
	catalyst_3850-nm-8-10g	1153
	catalyst_8200	1155
	catalyst_8300	1158
	catalyst_8300-1n1s-4t2x	1161
	catalyst_8300-1n1s-6t	1164
	catalyst_8300-2n2s-4t2x	1167
	catalyst_8300-2n2s-6t	1170
	catalyst_8500	1173
	catalyst_8500-4qc	1175
	catalyst_8500l	1178
	catalyst_8510csr	1182
	catalyst_8510msr	1185
	catalyst_8540csr	1188
	catalyst_8540msr	1191

Vendor	Product	Page Number
Cisco	catalyst_9100	1194
	catalyst_9105	1195
	catalyst_9105ax	1195
	catalyst_9105axi	1196
	catalyst_9105axw	1197
	catalyst_9115	1197
	catalyst_9115ax	1198
	catalyst_9115axe	1199
	catalyst_9115axi	1199
	catalyst_9115_ap	1200
	catalyst_9117	1201
	catalyst_9117ax	1201
	catalyst_9117axi	1202
	catalyst_9117_ap	1203
	catalyst_9120	1203
	catalyst_9120ax	1204
	catalyst_9120axe	1205
	catalyst_9120axi	1205
	catalyst_9120axp	1206
	catalyst_9120_ap	1207
	catalyst_9124	1207
	catalyst_9124ax	1208
	catalyst_9124axd	1209
	catalyst_9124axi	1209
	catalyst_9130	1210
	catalyst_9130ax	1211
	catalyst_9130axe	1211
	catalyst_9130axi	1212
	catalyst_9130_ap	1213
	catalyst_9200	1213
	catalyst_9200cx	1216
	catalyst_9200l	1218

Vendor	Product	Page Number
Cisco	catalyst_9300	1220
	catalyst_9300-24p-a	1223
	catalyst_9300-24p-e	1227
	catalyst_9300-24s-a	1230
	catalyst_9300-24s-e	1233
	catalyst_9300-24t-a	1237
	catalyst_9300-24t-e	1240
	catalyst_9300-24u-a	1243
	catalyst_9300-24u-e	1247
	catalyst_9300-24ux-a	1250
	catalyst_9300-24ux-e	1253
	catalyst_9300-48p-a	1257
	catalyst_9300-48p-e	1260
	catalyst_9300-48s-a	1263
	catalyst_9300-48s-e	1266
	catalyst_9300-48t-a	1270
	catalyst_9300-48t-e	1273
	catalyst_9300-48u-a	1276
	catalyst_9300-48u-e	1280
	catalyst_9300-48un-a	1283
	catalyst_9300-48un-e	1286
	catalyst_9300-48uxm-a	1290
	catalyst_9300-48uxm-e	1293
	catalyst_9300l	1296
	catalyst_9300l-24p-4g-a	1299
	catalyst_9300l-24p-4g-e	1303
	catalyst_9300l-24p-4x-a	1306
	catalyst_9300l-24p-4x-e	1309
	catalyst_9300l-24t-4g-a	1313
	catalyst_9300l-24t-4g-e	1316
	catalyst_9300l-24t-4x-a	1319
	catalyst_9300l-24t-4x-e	1323

Vendor	Product	Page Number
Cisco	catalyst_9300l-48p-4g-a	1326
	catalyst_9300l-48p-4g-e	1329
	catalyst_9300l-48p-4x-a	1332
	catalyst_9300l-48p-4x-e	1336
	catalyst_9300l-48t-4g-a	1339
	catalyst_9300l-48t-4g-e	1342
	catalyst_9300l-48t-4x-a	1346
	catalyst_9300l-48t-4x-e	1349
	catalyst_9300lm	1352
	catalyst_9300l_stack	1356
	catalyst_9300x	1359
	catalyst_9400	1362
	catalyst_9400_supervisor_engine-1	1364
	catalyst_9407r	1367
	catalyst_9410r	1369
	catalyst_9500	1371
	catalyst_9500h	1373
	catalyst_9600	1376
	catalyst_9600x	1378
	catalyst_9600_supervisor_engine-1	1380
	catalyst_9800	1382
	catalyst_9800-40	1385
	catalyst_9800-40_wireless_controller	1387
	catalyst_9800-80	1389
	catalyst_9800-80_wireless_controller	1391
	catalyst_9800-cl	1394
	catalyst_9800-l	1396
	catalyst_9800-l-c	1398
	catalyst_9800-l-f	1400
	catalyst_9800_embedded_wireless_controller	1403
	catalyst_ie3200	1405
	catalyst_ie3200_rugged_switch	1406

Vendor	Product	Page Number
hpe	aruba_cx_8320-32	1553
	aruba_cx_8320-48p	1554
	aruba_cx_8325-32c	1554
	aruba_cx_8325-48y8c	1554
	aruba_cx_8360-12c	1555
	aruba_cx_8360-16y2c	1555
	aruba_cx_8360-24xf2c	1556
	aruba_cx_8360-32y4c	1556
	aruba_cx_8360-48xt4c	1557
	aruba_cx_8360-48y6c	1557
	aruba_cx_8400	1558
	aruba_cx_9300_32d	1558
	edgeline_e920d_server_blade	1558
	edgeline_e920t_server_blade	1559
	edgeline_e920_server_blade	1559
	proliant_bl420c_gen8_server	1560
	proliant_bl460c_gen10_server_blade	1560
	proliant_bl460c_gen8_server_blade	1560
	proliant_bl460c_gen9_server_blade	1561
	proliant_bl465c_gen8_server_blade	1561
	proliant_bl660c_gen8_server_blade	1562
	proliant_bl660c_gen9_server	1562
	proliant_dl120_gen10_server	1562
	proliant_dl120_gen9_server	1563
	proliant_dl160_gen10_server	1563
	proliant_dl160_gen8_server	1564
	proliant_dl160_gen9_server	1564
	proliant_dl180_gen10_server	1564
	proliant_dl180_gen9_server	1565
	proliant_dl20_gen10_plus_server	1565
	proliant_dl20_gen10_server	1566
	proliant_dl20_gen9_server	1566

Vendor	Product	Page Number
hpe	proliant_sl250s_gen8_server	1592
	proliant_sl270s_gen8_server	1592
	proliant_sl270s_gen8_se_server	1593
	proliant_ws460c_gen8_graphics_server_blade	1593
	proliant_ws460c_gen9_graphics_server_blade	1594
	proliant_xl170r_gen10_server	1594
	proliant_xl170r_gen9_server	1594
	proliant_xl190r_gen10_server	1595
	proliant_xl190r_gen9_server	1595
	proliant_xl220a_gen8_v2_server	1596
	proliant_xl220n_gen10_plus_server	1596
	proliant_xl225n_gen10_plus_1u_node	1596
	proliant_xl230a_gen9_server	1597
	proliant_xl230b_gen9_server	1597
	proliant_xl230k_gen10_server	1598
	proliant_xl250a_gen9_server	1598
	proliant_xl270d_gen10_server	1598
	proliant_xl270d_gen9_special_server	1599
	proliant_xl290n_gen10_plus_server	1599
	proliant_xl450_gen10_server	1600
	proliant_xl450_gen9_server	1600
	proliant_xl645d_gen10_plus_server	1600
	proliant_xl675d_gen10_plus_server	1601
	proliant_xl730f_gen9_server	1601
	proliant_xl740f_gen9_server	1602
	proliant_xl750f_gen9_server	1602
	storage_file_controller	1602
	storage_performance_file_controller	1603
	storeeasy_1430_storage	1603
	storeeasy_1440_storage	1604
	storeeasy_1450_storage	1604
	storeeasy_1460_storage	1604

Vendor	Product	Page Number
hpe	storeeasy_1530_storage	1605
	storeeasy_1540_storage	1605
	storeeasy_1550_storage	1606
	storeeasy_1560_storage	1606
	storeeasy_1630_storage	1606
	storeeasy_1640_storage	1607
	storeeasy_1650_expanded_storage	1607
	storeeasy_1650_storage	1608
	storeeasy_1660_expanded_storage	1608
	storeeasy_1660_performance_storage	1608
	storeeasy_1660_storage	1609
	storeeasy_1830_storage	1609
	storeeasy_1840_storage	1610
	storeeasy_1850_storage	1610
	storeeasy_1860_performance_storage	1610
	storeeasy_1860_storage	1611
	storeeasy_3830_gateway_storage	1611
	storeeasy_3830_gateway_storage_blade	1612
	storeeasy_3840_gateway_storage	1612
	storeeasy_3840_gateway_storage_blade	1612
	storeeasy_3850_gateway_single_node_upgrade	1613
	storeeasy_3850_gateway_storage	1613
	storeeasy_3850_gateway_storage_blade	1614
	storevirtual_3000_file_controller	1614
	synergy_480_gen10_compute_module	1614
	synergy_480_gen10_plus_compute_module	1615
	synergy_480_gen9_compute_module	1615
	synergy_620_gen9_compute_module	1616
	synergy_660_gen10_compute_module	1616
	synergy_660_gen9_compute_module	1616
	synergy_680_gen9_compute_module	1617
jcgcn.com	jhr-n916r	1617

Vendor	Product	Page Number
lancombg	sa-wr915nd	1618
Omron	sysmac_cj2h-cpu64	1618
	sysmac_cj2h-cpu64-eip	1618
	sysmac_cj2h-cpu65	1619
	sysmac_cj2h-cpu65-eip	1619
	sysmac_cj2h-cpu66	1620
	sysmac_cj2h-cpu66-eip	1621
	sysmac_cj2h-cpu67	1621
	sysmac_cj2h-cpu67-eip	1622
	sysmac_cj2h-cpu68	1622
	sysmac_cj2h-cpu68-eip	1623
	sysmac_cj2m-cpu11	1623
	sysmac_cj2m-cpu12	1624
	sysmac_cj2m-cpu13	1624
	sysmac_cj2m-cpu14	1625
	sysmac_cj2m-cpu15	1626
	sysmac_cj2m-cpu31	1626
	sysmac_cj2m-cpu32	1627
	sysmac_cj2m-cpu33	1627
	sysmac_cj2m-cpu34	1628
	sysmac_cj2m-cpu35	1628
	sysmac_cp1e-e10dr-a	1629
	sysmac_cp1e-e10dr-d	1629
	sysmac_cp1e-e10dt-a	1630
	sysmac_cp1e-e10dt-d	1631
	sysmac_cp1e-e10dt1-a	1631
	sysmac_cp1e-e10dt1-d	1632
	sysmac_cp1e-e14dr-a	1632
	sysmac_cp1e-e14sdr-a	1633
	sysmac_cp1e-e20dr-a	1633
	sysmac_cp1e-e20sdr-a	1634
	sysmac_cp1e-e30dr-a	1634

Vendor	Product	Page Number
Omron	sysmac_cp1e-e30sdr-a	1635
	sysmac_cp1e-e40dr-a	1636
	sysmac_cp1e-e40sdr-a	1636
	sysmac_cp1e-e60sdr-a	1637
	sysmac_cp1e-na20dr-a	1637
	sysmac_cp1e-na20dt-d	1638
	sysmac_cp1e-na20dt1-d	1638
	sysmac_cp1h-x40dr-a	1639
	sysmac_cp1h-x40dt-d	1639
	sysmac_cp1h-x40dt1-d	1640
	sysmac_cp1h-xa40dr-a	1641
	sysmac_cp1h-xa40dt-d	1641
	sysmac_cp1h-xa40dt1-d	1642
	sysmac_cp1h-y20dt-d	1642
	sysmac_cp1l-el20dr-d	1643
	sysmac_cp1l-em30dr-d	1643
	sysmac_cp1l-em30dt-d	1644
	sysmac_cp1l-em30dt1-d	1644
	sysmac_cp1l-em40dr-d	1645
	sysmac_cp1l-em40dt-d	1646
	sysmac_cp1l-em40dt1-d	1646
	sysmac_cp1l-l10dr-a	1647
	sysmac_cp1l-l10dr-d	1647
	sysmac_cp1l-l10dt-a	1648
	sysmac_cp1l-l10dt-d	1648
	sysmac_cp1l-l10dt1-d	1649
	sysmac_cp1l-l14dr-a	1649
	sysmac_cp1l-l14dr-d	1650
	sysmac_cp1l-l14dt-a	1651
	sysmac_cp1l-l14dt-d	1651
	sysmac_cp1l-l14dt1-d	1652
	sysmac_cp1l-l20dr-a	1652

Vendor	Product	Page Number
Omron	sysmac_cp1l-l20dr-d	1653
	sysmac_cp1l-l20dt-a	1653
	sysmac_cp1l-l20dt-d	1654
	sysmac_cp1l-l20dt1-d	1654
	sysmac_cp1l-m30dr-a	1655
	sysmac_cp1l-m30dr-d	1656
	sysmac_cp1l-m30dt-a	1656
	sysmac_cp1l-m30dt-d	1657
	sysmac_cp1l-m30dt1-d	1657
	sysmac_cp1l-m40dr-a	1658
	sysmac_cp1l-m40dr-d	1658
	sysmac_cp1l-m40dt-a	1659
	sysmac_cp1l-m40dt-d	1659
	sysmac_cp1l-m40dt1-d	1660
	sysmac_cp1l-m60dr-a	1661
	sysmac_cp1l-m60dr-d	1661
	sysmac_cp1l-m60dt-a	1662
	sysmac_cp1l-m60dt-d	1662
	sysmac_cp1l-m60dt1-d	1663
	sysmac_cp2e-e14dr-a	1663
	sysmac_cp2e-e20dr-a	1664
	sysmac_cp2e-e30dr-a	1664
	sysmac_cp2e-e40dr-a	1665
	sysmac_cp2e-e60dr-a	1666
	sysmac_cp2e-n14dr-a	1666
	sysmac_cp2e-n14dr-d	1667
	sysmac_cp2e-n14dt-a	1667
	sysmac_cp2e-n14dt-d	1668
	sysmac_cp2e-n14dt1-d	1668
	sysmac_cp2e-n20dr-a	1669
	sysmac_cp2e-n20dr-d	1669
	sysmac_cp2e-n20dt-a	1670

Vendor	Product	Page Number
Omron	sysmac_cp2e-n20dt-d	1671
	sysmac_cp2e-n20dt1-d	1671
	sysmac_cp2e-n30dr-a	1672
	sysmac_cp2e-n30dr-d	1672
	sysmac_cp2e-n30dt-a	1673
	sysmac_cp2e-n30dt-d	1673
	sysmac_cp2e-n30dt1-d	1674
	sysmac_cp2e-n40dr-a	1674
	sysmac_cp2e-n40dr-d	1675
	sysmac_cp2e-n40dt-a	1676
	sysmac_cp2e-n40dt-d	1676
	sysmac_cp2e-n40dt1-d	1677
	sysmac_cp2e-n60dr-a	1677
	sysmac_cp2e-n60dr-d	1678
	sysmac_cp2e-n60dt-a	1678
	sysmac_cp2e-n60dt-d	1679
	sysmac_cp2e-n60dt1-d	1679
	sysmac_cp2e-s30dr-a	1680
	sysmac_cp2e-s30dt-d	1681
	sysmac_cp2e-s30dt1-d	1681
	sysmac_cp2e-s40dr-a	1682
	sysmac_cp2e-s40dt-d	1682
	sysmac_cp2e-s40dt1-d	1683
	sysmac_cp2e-s60dr-a	1683
	sysmac_cp2e-s60dt-d	1684
	sysmac_cp2e-s60dt1-d	1684
	sysmac_cs1w-drm21-v1	1685
	sysmac_cs1w-eip21	1686
	sysmac_cs1w-etn21	1686
	sysmac_cs1w-fln22	1687
	sysmac_cs1w-nc\[\]71	1687
	sysmac_cs1w-spu01-v2	1688

Vendor	Product	Page Number
Omron	sysmac_cp1e-e10dt-d_firmware	2349
	sysmac_cp1e-e10dt1-a_firmware	2350
	sysmac_cp1e-e10dt1-d_firmware	2350
	sysmac_cp1e-e14dr-a_firmware	2351
	sysmac_cp1e-e14sdr-a_firmware	2351
	sysmac_cp1e-e20dr-a_firmware	2352
	sysmac_cp1e-e20sdr-a_firmware	2353
	sysmac_cp1e-e30dr-a_firmware	2353
	sysmac_cp1e-e30sdr-a_firmware	2354
	sysmac_cp1e-e40dr-a_firmware	2354
	sysmac_cp1e-e40sdr-a_firmware	2355
	sysmac_cp1e-e60sdr-a_firmware	2355
	sysmac_cp1e-na20dr-a_firmware	2356
	sysmac_cp1e-na20dt-d_firmware	2356
	sysmac_cp1e-na20dt1-d_firmware	2357
	sysmac_cp1h-x40dr-a_firmware	2358
	sysmac_cp1h-x40dt-d_firmware	2358
	sysmac_cp1h-x40dt1-d_firmware	2359
	sysmac_cp1h-xa40dr-a_firmware	2359
	sysmac_cp1h-xa40dt-d_firmware	2360
	sysmac_cp1h-xa40dt1-d_firmware	2360
	sysmac_cp1h-y20dt-d_firmware	2361
	sysmac_cp1l-el20dr-d_firmware	2361
	sysmac_cp1l-em30dr-d_firmware	2362
	sysmac_cp1l-em30dt-d_firmware	2363
	sysmac_cp1l-em30dt1-d_firmware	2363
	sysmac_cp1l-em40dr-d_firmware	2364
	sysmac_cp1l-em40dt-d_firmware	2364
	sysmac_cp1l-em40dt1-d_firmware	2365
	sysmac_cp1l-l10dr-a_firmware	2365
	sysmac_cp1l-l10dr-d_firmware	2366
	sysmac_cp1l-l10dt-a_firmware	2366

Vendor	Product	Page Number
Omron	sysmac_cp1l-l10dt-d_firmware	2367
	sysmac_cp1l-l10dt1-d_firmware	2368
	sysmac_cp1l-l14dr-a_firmware	2368
	sysmac_cp1l-l14dr-d_firmware	2369
	sysmac_cp1l-l14dt-a_firmware	2369
	sysmac_cp1l-l14dt-d_firmware	2370
	sysmac_cp1l-l14dt1-d_firmware	2370
	sysmac_cp1l-l20dr-a_firmware	2371
	sysmac_cp1l-l20dr-d_firmware	2371
	sysmac_cp1l-l20dt-a_firmware	2372
	sysmac_cp1l-l20dt-d_firmware	2373
	sysmac_cp1l-l20dt1-d_firmware	2373
	sysmac_cp1l-m30dr-a_firmware	2374
	sysmac_cp1l-m30dr-d_firmware	2374
	sysmac_cp1l-m30dt-a_firmware	2375
	sysmac_cp1l-m30dt-d_firmware	2375
	sysmac_cp1l-m30dt1-d_firmware	2376
	sysmac_cp1l-m40dr-a_firmware	2376
	sysmac_cp1l-m40dr-d_firmware	2377
	sysmac_cp1l-m40dt-a_firmware	2378
	sysmac_cp1l-m40dt-d_firmware	2378
	sysmac_cp1l-m40dt1-d_firmware	2379
	sysmac_cp1l-m60dr-a_firmware	2379
	sysmac_cp1l-m60dr-d_firmware	2380
	sysmac_cp1l-m60dt-a_firmware	2380
	sysmac_cp1l-m60dt-d_firmware	2381
	sysmac_cp1l-m60dt1-d_firmware	2381
	sysmac_cp2e-e14dr-a_firmware	2382
	sysmac_cp2e-e20dr-a_firmware	2383
	sysmac_cp2e-e30dr-a_firmware	2383
	sysmac_cp2e-e40dr-a_firmware	2384
	sysmac_cp2e-e60dr-a_firmware	2384

Vendor	Product	Page Number
Omron	sysmac_cp2e-n14dr-a_firmware	2385
	sysmac_cp2e-n14dr-d_firmware	2385
	sysmac_cp2e-n14dt-a_firmware	2386
	sysmac_cp2e-n14dt-d_firmware	2386
	sysmac_cp2e-n14dt1-d_firmware	2387
	sysmac_cp2e-n20dr-a_firmware	2388
	sysmac_cp2e-n20dr-d_firmware	2388
	sysmac_cp2e-n20dt-a_firmware	2389
	sysmac_cp2e-n20dt-d_firmware	2389
	sysmac_cp2e-n20dt1-d_firmware	2390
	sysmac_cp2e-n30dr-a_firmware	2390
	sysmac_cp2e-n30dr-d_firmware	2391
	sysmac_cp2e-n30dt-a_firmware	2391
	sysmac_cp2e-n30dt-d_firmware	2392
	sysmac_cp2e-n30dt1-d_firmware	2393
	sysmac_cp2e-n40dr-a_firmware	2393
	sysmac_cp2e-n40dr-d_firmware	2394
	sysmac_cp2e-n40dt-a_firmware	2394
	sysmac_cp2e-n40dt-d_firmware	2395
	sysmac_cp2e-n40dt1-d_firmware	2395
	sysmac_cp2e-n60dr-a_firmware	2396
	sysmac_cp2e-n60dr-d_firmware	2396
	sysmac_cp2e-n60dt-a_firmware	2397
	sysmac_cp2e-n60dt-d_firmware	2398
	sysmac_cp2e-n60dt1-d_firmware	2398
	sysmac_cp2e-s30dr-a_firmware	2399
	sysmac_cp2e-s30dt-d_firmware	2399
	sysmac_cp2e-s30dt1-d_firmware	2400
	sysmac_cp2e-s40dr-a_firmware	2400
	sysmac_cp2e-s40dt-d_firmware	2401
	sysmac_cp2e-s40dt1-d_firmware	2401
	sysmac_cp2e-s60dr-a_firmware	2402

Vendor	Product	Page Number
Samsung	exynos_modem_5123_firmware	2435
	exynos_modem_5300_firmware	2436
sauter-controls	ey-as525f001_firmware	2437
silabs	wireless_smart_ubiquitous_network_linux_border_router_firmware	2439
Tenda	ax3_firmware	2439
	g103_firmware	2439
	w20e_firmware	2439
totolink	a7100ru_firmware	2440
Tp-link	tl-mr3020_firmware	2440
ui	edgerouter_x_firmware	2441

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: accesspressthemes					
Product: smart_logo_showcase_lite					
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/1
Affected Version(s): 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform	N/A	A-ACC-SMAR-050423/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/3
Affected Version(s): 1.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-ACC-SMAR-050423/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0175		
Affected Version(s): 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/5
Affected Version(s): 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/7
Affected Version(s): 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/8
Affected Version(s): 1.0.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/9
Affected Version(s): 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/10
Affected Version(s): 1.1.0					
Improper Neutralizat	20-Mar-2023	5.4	The Responsive Clients Logo Gallery	N/A	A-ACC-SMAR-050423/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/12
Affected Version(s): 1.1.2					
Improper Neutralization of Input	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9	N/A	A-ACC-SMAR-050423/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/14
Affected Version(s): 1.1.4					
Improper Neutralization of Input During Web Page	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its	N/A	A-ACC-SMAR-050423/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/16
Affected Version(s): 1.1.6					
Improper Neutralization of Input During Web Page Generation	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting	N/A	A-ACC-SMAR-050423/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/18
Affected Version(s): 1.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the	N/A	A-ACC-SMAR-050423/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**		
Affected Version(s): 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0175**	N/A	A-ACC-SMAR-050423/20
Product: wp_popup_banners					
Affected Version(s): 1.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action.	N/A	A-ACC-WP_P-050423/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28661		
Affected Version(s): 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/22
Affected Version(s): 1.0.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/23
Affected Version(s): 1.0.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/25
Affected Version(s): 1.0.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/26
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/27
Affected Version(s): 1.0.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/28
Affected Version(s): 1.0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/29
Affected Version(s): 1.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/30
Affected Version(s): 1.1.1					
Improper Neutralizat	22-Mar-2023	8.8	The WP Popup Banners WordPress	N/A	A-ACC-WP_P-050423/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**		
Affected Version(s): 1.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/32
Affected Version(s): 1.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/33
Affected Version(s): 1.1.4					
Improper Neutralization of Special	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an	N/A	A-ACC-WP_P-050423/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**		
Affected Version(s): 1.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/35
Affected Version(s): 1.1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/36
Affected Version(s): 1.1.7					
Improper Neutralization of Special Elements used in an	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability	N/A	A-ACC-WP_P-050423/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**		
Affected Version(s): 1.1.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/38
Affected Version(s): 1.1.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/39
Affected Version(s): 1.2.0					
Improper Neutralization of Special Elements used in an SQL Command	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the	N/A	A-ACC-WP_P-050423/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			get_popup_data action. **CVE ID : CVE-2023-28661**		
Affected Version(s): 1.2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/41
Affected Version(s): 1.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/42
Affected Version(s): 1.2.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action.	N/A	A-ACC-WP_P-050423/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28661		
Affected Version(s): 1.2.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/44
Affected Version(s): 1.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. **CVE ID : CVE-2023-28661**	N/A	A-ACC-WP_P-050423/45
Vendor: admin_log_project					
Product: admin_log					
Affected Version(s): * Up to (including) 1.50					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in David Gwyer Admin Log plugin <= 1.50 versions. **CVE ID : CVE-2023-23721**	N/A	A-ADM-ADMI-050423/46
Vendor: Adobe					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: coldfusion					
Affected Version(s): 2018					
Deserialization of Untrusted Data	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26359**	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	A-ADO-COLD-050423/47
Improper Access Control	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26360**	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	A-ADO-COLD-050423/48
Improper Limitation of a Pathname to a	23-Mar-2023	4.9	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by	https://helpx.adobe.com/security/products/coldfusion/	A-ADO-COLD-050423/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in Arbitrary file system read. Exploitation of this issue does not require user interaction, but does require administrator privileges. **CVE ID : CVE-2023-26361**	apsb23-25.html	
Affected Version(s): 2021					
Deserialization of Untrusted Data	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26359**	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	A-ADO-COLD-050423/50
Improper Access Control	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	A-ADO-COLD-050423/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26360**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	4.9	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in Arbitrary file system read. Exploitation of this issue does not require user interaction, but does require administrator privileges. **CVE ID : CVE-2023-26361**	https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html	A-ADO-COLD-050423/52
Product: creative_cloud					
Affected Version(s): * Up to (excluding) 5.10					
Untrusted Search Path	22-Mar-2023	7.8	Creative Cloud version 5.9.1 (and earlier) is affected by an Untrusted Search Path vulnerability that might allow attackers to execute their own programs, access unauthorized data	https://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html	A-ADO-CREA-050423/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files, or modify configuration in unexpected ways. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. The problem extends to any type of critical resource that the application trusts. **CVE ID : CVE-2023-26358**		
Product: dimension					
Affected Version(s): * Up to (excluding) 3.4.8					
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25903**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/54
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of	https://helpx.adobe.com/security/products/	A-ADO-DIME-050423/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26334**	dimension/apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26335**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/56
Use After Free	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26336**		
Out-of-bounds Write	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26337**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/58
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26338**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26339**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/60
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26340**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/61
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that	https://helpx.adobe.com/security/products/dimension/	A-ADO-DIME-050423/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26341**	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26342**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/63
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26343**		
Access of Uninitialized Pointer	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26344**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/65
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26345**		
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26346**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/67
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26348		
Use After Free	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26349**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/69
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26350**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26351**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/71
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26352**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/72
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that	https://helpx.adobe.com/security/products/dimension/	A-ADO-DIME-050423/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26353**	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26354**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/74
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26355**		
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26356**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/76
Product: experience_manager					
Affected Version(s): * Up to (excluding) 6.5.16.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-21615**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-21616**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22252**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22253**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/80
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22254**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/81
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-	https://helpx.adobe.com/security/products/experience-manager/a	A-ADO-EXPE-050423/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22256**	psb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22257**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/83
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction. **CVE ID : CVE-2023-22258**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22259**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/85
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22260**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/86
URL Redirectio	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	https://helpx.adobe.co	A-ADO-EXPE-050423/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22261**	m/security/products/experience-manager/apsb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22262**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/88
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22263**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22264**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/90
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction. **CVE ID : CVE-2023-22265**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22266**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22269**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	22-Mar-2023	5.3	Experience Manager versions 6.5.15.0 (and earlier) are affected by a Weak Cryptography for Passwords vulnerability that can lead to a security feature bypass. A low-privileged attacker can exploit this in order to decrypt a user's password. The attack complexity is high since a successful exploitation requires to already have in possession this encrypted secret. **CVE ID : CVE-2023-22271**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/94
Product: experience_manager_cloud_service					
Affected Version(s): * Up to (excluding) 2023.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-21615**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/95
Improper Neutralizat	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	https://helpx.adobe.co	A-ADO-EXPE-050423/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-21616**	m/security/products/experience-manager/apsb23-18.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22252**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/97
Improper Neutralization of Input During Web Page Generation	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22253**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22254**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/99
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction. **CVE ID : CVE-2023-22256**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22257**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/101
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22258**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/102
URL Redirectio	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	https://helpx.adobe.co	A-ADO-EXPE-050423/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22259**	m/security/products/experience-manager/apsb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22260**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/104
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22261**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22262**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/106
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction. **CVE ID : CVE-2023-22263**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22264**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/108
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22265**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/109
URL Redirectio	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	https://helpx.adobe.co	A-ADO-EXPE-050423/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2023-22266**	m/security/products/experience-manager/apsb23-18.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-22269**	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/111
Inadequate Encryption Strength	22-Mar-2023	5.3	Experience Manager versions 6.5.15.0 (and earlier) are affected by a Weak Cryptography for Passwords vulnerability that can lead to a security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html	A-ADO-EXPE-050423/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can exploit this in order to decrypt a user's password. The attack complexity is high since a successful exploitation requires to already have in possession this encrypted secret. **CVE ID : CVE-2023-22271**		
Product: illustrator					
Affected Version(s): * Up to (including) 26.5.2					
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25859**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/113
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25860**		
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25861**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/115
Use After Free	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26426**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-Mar-2023	5.5	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25862**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/117
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.3.1					
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25859**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/118
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and	https://helpx.adobe.com/security	A-ADO-ILLU-050423/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25860**	/products/illustrator/apsb23-19.html	
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25861**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/120
Use After Free	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26426**		
Out-of-bounds Read	22-Mar-2023	5.5	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25862**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	A-ADO-ILLU-050423/122
Vendor: air_cargo_management_system_project					
Product: air_cargo_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability was found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/transactions/update_status.php of the component GET Parameter Handler. The manipulation of	N/A	A-AIR-AIR_-050423/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the argument id 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-223556. **CVE ID : CVE-2023-1564**		
Vendor: alphaware_-_simple_e-commerce_system_project					
Product: alphaware_-_simple_e-commerce_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file function/edit_customer.php. The manipulation of the argument firstname/mi/lastname with the input a' RLIKE SLEEP(5) AND 'dAbu'='dAbu leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-223406 is the identifier assigned to this vulnerability.	N/A	A-ALP-ALPH-050423/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1502		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E-Commerce System 1.0. This affects an unknown part of the file admin/admin_index.php. The manipulation of the argument username/password with the input admin' AND (SELECT 8062 FROM (SELECT(SLEEP(5)))meUD)-- hLiX 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-223407. **CVE ID : CVE-2023-1503**	N/A	A-ALP-ALPH-050423/125
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Alphaware Simple E-Commerce System 1.0. This vulnerability affects unknown code. The manipulation of the argument email/password with the input	N/A	A-ALP-ALPH-050423/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test1%40test.com ' AND (SELECT 6077 FROM (SELECT(SLEEP(5)))dltn) AND 'PhRa'='PhRa leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223408. **CVE ID : CVE-2023-1504**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	9.8	An issue was discovered in Alphaware - Simple E-Commerce System v1.0. There is a SQL injection that can directly issue instructions to the background database system via /alphaware/details.php?id. **CVE ID : CVE-2023-26905**	N/A	A-ALP-ALPH-050423/127
Vendor: altanic					
Product: no_api_amazon_affiliate					
Affected Version(s): * Up to (including) 4.2.2					
Improper Neutralization of Input During Web Page Generation	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Altanic No API Amazon Affiliate plugin <= 4.2.2 versions.	N/A	A-ALT-NO_A-050423/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-22680**		
Vendor: amano					
Product: xoffice					
Affected Version(s): 7.1.3879					
Files or Directories Accessible to External Parties	28-Mar-2023	7.5	amano Xparc parking solutions 7.1.3879 was discovered to be vulnerable to local file inclusion. **CVE ID : CVE-2023-23330**	N/A	A-AMA-XOFF-050423/129
Vendor: ansible-semaphore					
Product: ansible_semaphore					
Affected Version(s): * Up to (excluding) 2.8.89					
Improper Authentication	18-Mar-2023	9.8	api/auth.go in Ansible Semaphore before 2.8.89 mishandles authentication. **CVE ID : CVE-2023-28609**	https://github.com/ansible-semaphore/semaphore/commit/3e4a62b7f2b1ef0660c9fb839818a53c80a5a8b1	A-ANS-ANSI-050423/130
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.0.6					
Authentication Bypass by Capture-replay	21-Mar-2023	9.8	Authentication Bypass by Capture-replay in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1537**	https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af, https://hu	A-ANS-ANSW-050423/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ntr.dev/bounties/171cde18-a447-446c-a9ab-297953ad9b86	
Insufficient Session Expiration	21-Mar-2023	8.8	Insufficient Session Expiration in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1543**	https://github.com/answerdev/answer/commit/cd742b75605c99776f32d271c0a60e0f468e181c, https://huntr.dev/bounties/f82388d6-dfc3-4fbc-bea6-eb40cf5b2683	A-ANS-ANSW-050423/132
N/A	21-Mar-2023	5.4	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1542**	https://github.com/answerdev/answer/commit/4ca2429d190a6e614f5bbee1173c80a7cffcc568, https://huntr.dev/bounties/d947417c-5a12-407a-9a2f-fa696f65126f	A-ANS-ANSW-050423/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	21-Mar-2023	5.3	Observable Timing Discrepancy in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1538**	https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af, https://huntr.dev/bounties/ac0271eb-660f-4966-8b57-4bc660a9a1a0	A-ANS-ANSW-050423/134
Improper Restriction of Excessive Authentication Attempts	21-Mar-2023	5.3	Guessable CAPTCHA in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1539**	https://huntr.dev/bounties/b4df67f4-14ea-4051-97d4-26690c979a28, https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af	A-ANS-ANSW-050423/135
Observable Discrepancy	21-Mar-2023	5.3	Observable Response Discrepancy in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1540**	https://huntr.dev/bounties/d8d6c259-a0f2-4209-a3b0-ecbf3eb092f4, https://git	A-ANS-ANSW-050423/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				hub.com/answerdev/answer/commit/1de3ec27e50ba7389c9449c59e8ea3a37a908ee4	
N/A	21-Mar-2023	3.8	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1541**	https://github.com/answerdev/answer/commit/15390adbfcd5fd37af4661f992f8873ae5a6b840, https://huntr.dev/bounties/8fd891c6-b04e-4dac-818f-9ea30861cd92	A-ANS-ANSW-050423/137
Affected Version(s): * Up to (excluding) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7. **CVE ID : CVE-2023-1535**	https://huntr.dev/bounties/4d4b0caa-6d8c-4574-ae7e-e9ef5e2e1a40, https://github.com/answerdev/answer/commit/c3743bad4f2a69f69f8f1e1e5b4b6524fc03da25	A-ANS-ANSW-050423/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7. **CVE ID : CVE-2023-1536**	https://huntr.dev/bounties/538207f4-f805-419a-a314-51716643f05e, https://github.com/answerdev/answer/commit/c3743bad4f2a69f69f8f1e1e5b4b6524fc03da25	A-ANS-ANSW-050423/139
Vendor: Apache					
Product: fineract					
Affected Version(s): From (including) 1.4.0 Up to (including) 1.8.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Mar-2023	6.3	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation apache fineract. Authorized users may be able to exploit this for limited impact on components. This issue affects apache fineract: from 1.4 through 1.8.2. **CVE ID : CVE-2023-25197**	https://lists.apache.org/thread/v0q9x86sx6f6l2nzr1z0nwm3y9qlng04	A-APA-FINE-050423/140
Improper Neutralization of Special	28-Mar-2023	4.3	Improper Neutralization of Special Elements used in an SQL Command	https://lists.apache.org/thread/m9x3vpn3	A-APA-FINE-050423/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			('SQL Injection') vulnerability in Apache Software Foundation Apache Fineract. Authorized users may be able to change or add data in certain components. This issue affects Apache Fineract: from 1.4 through 1.8.2. **CVE ID : CVE-2023-25196**	bry4fympkzxnnz4qx0oc0w8m	
Affected Version(s): From (including) 1.4.0 Up to (including) 1.8.3					
Server-Side Request Forgery (SSRF)	28-Mar-2023	8.1	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache Fineract. Authorized users with limited permissions can gain access to server and may be able to use server for any outbound traffic. This issue affects Apache Fineract: from 1.4 through 1.8.3. **CVE ID : CVE-2023-25195**	https://lists.apache.org/thread/m58fdjmtkfp9h4c0r4l48rv995w3qhb6	A-APA-FINE-050423/142
Product: inlong					
Affected Version(s): From (including) 1.1.0 Up to (including) 1.5.0					
Deserialization of Untrusted Data	27-Mar-2023	8.8	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong. It could be triggered by authenticated users of InLong, you could	https://lists.apache.org/thread/xbvtjw9bwzgbo9fp1by8o3p49nf59xzt	A-APA-INLO-050423/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refer to [1] to know more about this vulnerability. This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick [2] to solve it. [1] https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html [2] https://github.com/apache/inlong/pull/7422 https://github.com/apache/inlong/pull/7422 **CVE ID : CVE-2023-27296**		
Product: sling_resource_merger					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.4.2					
Excessive Iteration	20-Mar-2023	7.5	Excessive Iteration vulnerability in Apache Software Foundation Apache Sling Resource Merger.This issue affects Apache Sling Resource Merger: from 1.2.0 before 1.4.2.	https://lists.apache.org/thread/xpcpo1y88ldss5hgmvogsf6h3735l5zb	A-APA-SLIN-050423/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26513		
Product: tomcat					
Affected Version(s): 11.0.0					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. **CVE ID : CVE-2023-28708**	https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67	A-APA-TOMC-050423/145
Affected Version(s): From (excluding) 10.1.0 Up to (excluding) 10.1.6					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute.	https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67	A-APA-TOMC-050423/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could result in the user agent transmitting the session cookie over an insecure channel. **CVE ID : CVE-2023-28708**		
Affected Version(s): From (excluding) 9.0.0 Up to (excluding) 9.0.72					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. **CVE ID : CVE-2023-28708**	https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67	A-APA-TOMC-050423/147
Affected Version(s): From (including) 8.5.0 Up to (excluding) 8.5.86					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1	https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67	A-APA-TOMC-050423/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. **CVE ID : CVE-2023-28708**		
Vendor: apiman					
Product: apiman					
Affected Version(s): 3.0.0					
Missing Authorization	27-Mar-2023	3.1	Apiman is a flexible and open source API Management platform. Due to a missing permissions check, an attacker with an authenticated Apiman Manager account may be able to gain access to API keys they do not have permission for if they correctly guess the URL, which includes Organisation ID, Client ID, and Client Version of the targeted non-permitted resource. While not trivial to exploit, it could be achieved by brute-forcing or guessing common names. Access to the non-permitted API Keys could allow use of other users' resources without their	https://github.com/apiman/apiman/security/advisories/GHSA-m6f8-hjrv-mw5f, https://www.apiman.io/blog/potential-permissions-bypass-disclosure/	A-API-APIM-050423/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission (depending on the specifics of configuration, such as whether an API key is the only form of security). Apiman 3.1.0.Final resolved this issue. Users are advised to upgrade. The only known workaround is to restrict account access. **CVE ID : CVE-2023-28640**		
Vendor: Arubanetworks					
Product: clearpass_policy_manager					
Affected Version(s): 6.11.0					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. **CVE ID : CVE-2023-25589**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/150
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-25594**		
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-25590**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/152
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. **CVE ID : CVE-2023-25591**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25592**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25593**		
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. **CVE ID : CVE-2023-25595**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/156
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ClearPass Policy Manager. **CVE ID : CVE-2023-25596**		
Affected Version(s): 6.11.1					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. **CVE ID : CVE-2023-25589**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/158
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorization on the platform. **CVE ID : CVE-2023-25594**		
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-25590**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/160
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. **CVE ID : CVE-2023-25591**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/161
Improper Neutralizat	22-Mar-2023	6.1	Vulnerabilities within the web-based	https://www.arubanet	A-ARU-CLEA-050423/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25592**	works.com/assets/alert/ARUBA-PSA-2023-003.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25593**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/163
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-CLEA-050423/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. **CVE ID : CVE-2023-25595**	PSA-2023-003.txt	
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager. **CVE ID : CVE-2023-25596**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/165
Affected Version(s): From (including) 6.10.0 Up to (including) 6.10.8					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the platform. A successful exploit allows an attacker to achieve total cluster compromise. **CVE ID : CVE-2023-25589**		
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-25594**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/167
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-25590**		
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. **CVE ID : CVE-2023-25591**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of the affected interface. **CVE ID : CVE-2023-25592**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25593**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/171
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25595		
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager. **CVE ID : CVE-2023-25596**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/173
Affected Version(s): From (including) 6.9.0 Up to (including) 6.9.13					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. **CVE ID : CVE-2023-25589**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/174
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy	https://www.arubanetworks.com/assets/ale	A-ARU-CLEA-050423/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-25594**	rt/ARUBA-PSA-2023-003.txt	
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-25590**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/176
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-CLEA-050423/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. **CVE ID : CVE-2023-25591**	PSA-2023-003.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25592**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/178
Improper Neutralization of Input During Web Page Generation	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-25593**		
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. **CVE ID : CVE-2023-25595**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/180
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			further access to network services supported by ClearPass Policy Manager. **CVE ID : CVE-2023-25596**		
Vendor: askoc					
Product: web_report_system					
Affected Version(s): * Up to (excluding) 23.03.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in As Koc Energy Web Report System allows SQL Injection.This issue affects Web Report System: before 23.03.10. **CVE ID : CVE-2023-1050**	N/A	A-ASK-WEB_-050423/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in As Koc Energy Web Report System allows Reflected XSS.This issue affects Web Report System: before 23.03.10. **CVE ID : CVE-2023-1051**	N/A	A-ASK-WEB_-050423/183
Vendor: automatic_question_paper_generator_system_project					
Product: automatic_question_paper_generator_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability has been found in SourceCodester Automatic Question Paper Generator System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/courses/view_course.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223285 was assigned to this vulnerability. **CVE ID : CVE-2023-1441**	N/A	A-AUT-AUTO-050423/184
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects unknown code of the file users/question_papers/manage_question_paper.php of the component GET	N/A	A-AUT-AUTO-050423/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223336. **CVE ID : CVE-2023-1474**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Automatic Question Paper Generator System 1.0. This affects an unknown part of the file classes/Users.php?f=save_ruser. The manipulation of the argument id/email leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223659. **CVE ID : CVE-2023-1591**	N/A	A-AUT-AUTO-050423/186
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects	N/A	A-AUT-AUTO-050423/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			unknown code of the file admin/courses/view_class.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-223660. **CVE ID : CVE-2023-1592**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Automatic Question Paper Generator System 1.0. Affected is an unknown function of the file users/user/manage_user.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. 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-223284. **CVE ID : CVE-2023-1440**	N/A	A-AUT-AUTO-050423/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Automatic Question Paper Generator System 1.0. This issue affects some unknown processing of the file classes/Master.php?f=save_class. The manipulation of the argument description leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-223661 was assigned to this vulnerability. **CVE ID : CVE-2023-1593**	N/A	A-AUT-AUTO-050423/189
Vendor: Aver					
Product: ptzapp_2					
Affected Version(s): * Up to (excluding) 2.0.1051.53					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Mar-2023	7.5	Aver Information Inc PTZApp2 v20.01044.48 allows attackers to access sensitive files via a crafted GET request. **CVE ID : CVE-2023-27055**	N/A	A-AVE-PTZA-050423/190
Vendor: aveva					
Product: aveva_plant_scada					
Affected Version(s): 2020r2					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry	N/A	A-AVE-AVEV-050423/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states. **CVE ID : CVE-2023-1256**		
Affected Version(s): 2023					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states. **CVE ID : CVE-2023-1256**	N/A	A-AVE-AVEV-050423/192
Product: telemetry_server					
Affected Version(s): 2020r2					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states.	N/A	A-AVE-TELE-050423/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1256		
Vendor: awsm					
Product: embed_any_document					
Affected Version(s): * Up to (including) 2.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Unrestricted Upload of File with Dangerous Type vulnerability in Awsm Innovations Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files allows Stored XSS via upload of SVG and HTML files. This issue affects Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files plugin <= 2.7.1 versions. **CVE ID : CVE-2023-23707**	N/A	A-AWS-EMBE-050423/194
Vendor: Basercms					
Product: basercms					
Affected Version(s): * Up to (excluding) 4.7.5					
Unrestricted Upload of File with Dangerous Type	23-Mar-2023	9.8	baserCMS is a Content Management system. Prior to version 4.7.5, there is a Remote Code Execution (RCE) Vulnerability in the management system of baserCMS. Version 4.7.5 contains a patch.	https://github.com/baserproject/basercms/commit/60f83054d8131b0ace60716cec7e629b5eb3a8	A-BAS-BASE-050423/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25654	f0, https://github.com/baserproject/basercms/commit/002886be0998c74c386e04f0b43688a8a45d7a96	
Unrestricted Upload of File with Dangerous Type	23-Mar-2023	9.8	baserCMS is a Content Management system. Prior to version 4.7.5, any file may be uploaded on the management system of baserCMS. Version 4.7.5 contains a patch. **CVE ID : CVE-2023-25655**	https://github.com/baserproject/basercms/commit/9297629983ed908c7f51bf61a0231dde91404ebd, https://github.com/baserproject/basercms/commit/922025a98b0e697ab78f6a785a004e0729aa9100	A-BAS-BASE-050423/196
Vendor: basixonline					
Product: nex-forms					
Affected Version(s): * Up to (excluding) 8.3.3					
Improper Neutralization of Input During Web Page Generation	27-Mar-2023	5.4	The NEX-Forms WordPress plugin before 8.3.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where	N/A	A-BAS-NEX--050423/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0272**		
Vendor: booking-wp-plugin					
Product: bookly					
Affected Version(s): * Up to (excluding) 21.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	6.1	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the full name value in versions up to, and including, 21.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1172**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2876981%40bookly-responsive-appointment-booking-tool&new=2876981%40bookly-responsive-appointment-booking-tool&sfp_email=&sfph_mail=	A-BOO-BOOK-050423/198
Vendor: Broadcom					
Product: tcpreplay					
Affected Version(s): 4.4.3					
Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPreplay tcprewrite v.4.4.3 allows a remote attacker to	https://github.com/appneta/tcpreplay/pull	A-BRO-TCPR-050423/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service via the tcpedit_dlt_cleanup function at plugins/dlt_plugins.c. **CVE ID : CVE-2023-27783**	/781, https://github.com/appneta/tcpreplay/issues/780	
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPReplay v.4.4.3 allows a remote attacker to cause a denial of service via the read_hexstring function at the utils.c:309 endpoint. **CVE ID : CVE-2023-27784**	https://github.com/appneta/tcpreplay/issues/787	A-BRO-TCPR-050423/200
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPreplay TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the parse endpoints function. **CVE ID : CVE-2023-27785**	https://github.com/appneta/tcpreplay/issues/785	A-BRO-TCPR-050423/201
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the macinstring function. **CVE ID : CVE-2023-27786**	https://github.com/appneta/tcpreplay/pull/783, https://github.com/appneta/tcpreplay/issues/782	A-BRO-TCPR-050423/202
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the	https://github.com/appneta/tcpreplay/issues/788	A-BRO-TCPR-050423/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parse_list function at the list.c:81 endpoint. **CVE ID : CVE-2023-27787**		
Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPrewrite v.4.4.3 allows a remote attacker to cause a denial of service via the ports2PORT function at the portmap.c:69 endpoint. **CVE ID : CVE-2023-27788**	https://github.com/appneta/tcpreplay/issues/786	A-BRO-TCPR-050423/204
Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the cidr2cidr function at the cidr.c:178 endpoint. **CVE ID : CVE-2023-27789**	https://github.com/appneta/tcpreplay/pull/783, https://github.com/appneta/tcpreplay/issues/784	A-BRO-TCPR-050423/205
Vendor: cal					
Product: cal.com					
Affected Version(s): * Up to (excluding) 2.7.0					
N/A	27-Mar-2023	8.8	Improper Access Control in GitHub repository calcom/cal.com prior to 2.7. **CVE ID : CVE-2023-1647**	https://huntr.dev/bounties/d6de3d6e-9551-47d1-b28c-7e965c1b82b6, https://github.com/calcom/cal.com/commit/c76e5f461	A-CAL-CAL.-050423/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				01a826b2de39123c22f50c840dddba0	
Vendor: canteen_management_system_project					
Product: canteen_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file changeUsername.php. The manipulation of the argument username 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-223304. **CVE ID : CVE-2023-1459**	N/A	A-CAN-CANT-050423/207
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file createCategories.php. The manipulation of the argument	N/A	A-CAN-CANT-050423/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			categoriesStatus leads to sql injection. The attack can be initiated remotely. VDB-223306 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1461**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Canteen Management System 1.0. This issue affects the function query of the file createuser.php. The manipulation of the argument uemail 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-223337 was assigned to this vulnerability. **CVE ID : CVE-2023-1475**	N/A	A-CAN-CANT-050423/209
Vendor: cerebrate-project					
Product: cerebrate					
Affected Version(s): 1.13					
Improper Neutralization of Special Elements used in an SQL	27-Mar-2023	9.8	In Cerebrate 1.13, a blind SQL injection exists in the searchAll API endpoint. **CVE ID : CVE-2023-28883**	https://github.com/cerebrate-project/cerebrate/commit/5f1c99cd534442e	A-CER-CERE-050423/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')				c40c2129769608e3e61ff8be3	
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	RESERVED churchcrm v4.5.3 was discovered to contain a SQL injection vulnerability via the Event parameter at /churchcrm/EventAttendance.php. **CVE ID : CVE-2023-24787**	N/A	A-CHU-CHUR-050423/211
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	A cross-site scripting (XSS) vulnerability in the Edit Group function of ChurchCRM v4.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit Group Name text field. **CVE ID : CVE-2023-27059**	https://github.com/ChurchCRM/CRM/issues/6450	A-CHU-CHUR-050423/212
Vendor: cilium					
Product: cilium					
Affected Version(s): * Up to (excluding) 1.11.15					
Incorrect Authorization	17-Mar-2023	7.3	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1,	N/A	A-CIL-CILI-050423/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing. **CVE ID : CVE-2023-27594**		
Incorrect Default Permissions	17-Mar-2023	5.5	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can write to `/opt/cni/bin`	N/A	A-CIL-CILI-050423/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible. **CVE ID : CVE-2023-27593**		
Affected Version(s): 1.13.0					
Improper Handling of Exceptional Conditions	17-Mar-2023	9.8	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In version 1.13.0, when Cilium is started, there is a short period when	N/A	A-CIL-CILI-050423/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cilium eBPF programs are not attached to the host. During this period, the host does not implement any of Cilium's featureset. This can cause disruption to newly established connections during this period due to the lack of Load Balancing, or can cause Network Policy bypass due to the lack of Network Policy enforcement during the window. This vulnerability impacts any Cilium-managed endpoints on the node (such as Kubernetes Pods), as well as the host network namespace (including Host Firewall). This vulnerability is fixed in Cilium 1.13.1 or later. Cilium releases 1.12.x, 1.11.x, and earlier are not affected. There are no known workarounds. **CVE ID : CVE-2023-27595**		
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.8					
Incorrect Authorization	17-Mar-2023	7.3	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15,	N/A	A-CIL-CILI-050423/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.12.8, and 1.13.1, under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing. **CVE ID : CVE-2023-27594**		
Incorrect Default Permissions	17-Mar-2023	5.5	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can	N/A	A-CIL-CILI-050423/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to `/opt/cni/bin` due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible. **CVE ID : CVE-2023-27593**		
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.1					
Incorrect Authorization	17-Mar-2023	7.3	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1,	N/A	A-CIL-CILI-050423/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing. **CVE ID : CVE-2023-27594**		
Incorrect Default Permissions	17-Mar-2023	5.5	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can write to `/opt/cni/bin`	N/A	A-CIL-CILI-050423/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible. **CVE ID : CVE-2023-27593**		
Product: cilium-cli					
Affected Version(s): * Up to (excluding) 0.13.2					
Improper Handling of Insufficient Permissions or Privileges	22-Mar-2023	4.1	`cilium-cli` is the command line interface to install, manage, and troubleshoot Kubernetes clusters running Cilium. Prior to version	https://github.com/cilium/cilium-cli/security/advisories/GHSA-6f27-3p6c-	A-CIL-CILI-050423/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.13.2,`cilium-cli`, when used to configure cluster mesh functionality, can remove the enforcement of user permissions on the `etcd` store used to mirror local cluster information to remote clusters. Users who have set up cluster meshes using the Cilium Helm chart are not affected by this issue. Due to an incorrect mount point specification, the settings specified by the `initContainer` that configures `etcd` users and their permissions are overwritten when using `cilium-cli` to configure a cluster mesh. An attacker who has already gained access to a valid key and certificate for an `etcd` cluster compromised in this manner could then modify state in that `etcd` cluster. This issue is patched in `cilium-cli` 0.13.2. As a workaround, one may use Cilium's Helm charts to create their cluster. **CVE ID : CVE-2023-28114**	p5jc, https://github.com/cilium/cilium-cli/commit/fb1427025764e1eebc4a7710d902c4f22cae2610	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Cisco					
Product: adaptive_security_appliance					
Affected Version(s): 9.10.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.42					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.10.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.2.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.3.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.3.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.3.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.12.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.13.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.1.6					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.2.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.14.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.15.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.1.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.2.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.2.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.16.2.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.17.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.38					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.3.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.34					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.39					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.41					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.43					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.8.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.1.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.235					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.36					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.47					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.50					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.52					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.56					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.59					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.61					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.66					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.67					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.74					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.80					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.83					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.85					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Affected Version(s): 9.9.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-ADAP-050423/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: aironet_access_point_software					
Affected Version(s): * Up to (excluding) 17.9.0.135					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	A-CIS-AIRO-050423/380
Product: catalyst_8000v_edge					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	A-CIS-CATA-050423/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	rityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
Product: dna_center					
Affected Version(s): * Up to (excluding) 2.3.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	8.8	A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials. **CVE ID : CVE-2023-20055**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS	A-CIS-DNA_-050423/382
Affected Version(s): * Up to (excluding) 2.3.3.7					
Cleartext Storage of Sensitive Information	23-Mar-2023	6.5	A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-DNA_-050423/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view sensitive information in clear text, which could include configuration files. **CVE ID : CVE-2023-20059**	dnac-infodisc-pe7zAbdR	
Affected Version(s): 2.3.4.0					
N/A	23-Mar-2023	8.8	A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS	A-CIS-DNA_-050423/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials. **CVE ID : CVE-2023-20055**		
Affected Version(s): From (including) 2.3.4.0 Up to (excluding) 2.3.5.0					
Cleartext Storage of Sensitive Information	23-Mar-2023	6.5	A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-pe7zAbdR	A-CIS-DNA_-050423/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information in clear text, which could include configuration files. **CVE ID : CVE-2023-20059**		
Product: firepower_threat_defense					
Affected Version(s): 9.10.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.42					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.10.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.2.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.3.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.3.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.3.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.12.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.13.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.1.6					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.2.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.14.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.15.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.1.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.2.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.2.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.16.2.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.17.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.38					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.3.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.34					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.39					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.41					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.43					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.8.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.1.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.235					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.36					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.47					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.50					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.52					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.56					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.59					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.61					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.66					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.67					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.74					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.80					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.83					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.85					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): 9.9.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	A-CIS-FIRE-050423/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: wireless_lan_controller_software					
Affected Version(s): * Up to (excluding) 8.10.183.0					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	A-CIS-WIRE-050423/545
Vendor: Ckeditor					
Product: ckeditor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0 Up to (excluding) 4.21.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered affecting Iframe Dialog and Media Embed packages. The vulnerability may trigger a JavaScript code after fulfilling special conditions: using one of the affected packages on a web page with missing proper Content Security Policy configuration; initializing the editor on an element and using an element other than `<textarea>` as a base; and destroying the editor instance. This vulnerability might affect a small percentage of integrators that depend on dynamic editor initialization/destroy mechanism. A fix is available in CKEditor4 version 4.21.0. In some rare cases, a security fix may be considered a breaking change. Starting from version 4.21.0, the Iframe Dialog plugin applies the `sandbox`	https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-vh5c-xwqv-cv9g	A-CKE-CKED-050423/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attribute by default, which restricts JavaScript code execution in the iframe element. To change this behavior, configure the `config.iframe_attributes` option. Also starting from version 4.21.0, the Media Embed plugin regenerates the entire content of the embed widget by default. To change this behavior, configure the `config.embed_keepOriginalContent` option. Those who choose to enable either of the more permissive options or who cannot upgrade to a patched version should properly configure Content Security Policy to avoid any potential security issues that may arise from embedding iframe elements on their web page. **CVE ID : CVE-2023-28439**		
Vendor: cloudflare					
Product: cloudflared					
Affected Version(s): * Up to (excluding) 2023.3.1					
Improper Link Resolution Before File	21-Mar-2023	7.8	A vulnerability has been discovered in cloudflared's installer (<= 2023.3.0) for	https://github.com/cloudflare/cloudflared/s	A-CLO-CLOU-050423/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			Windows 32-bits devices that allows a local attacker with no administrative permissions to escalate their privileges on the affected device. This vulnerability exists because the MSI installer used by cloudflared relied on a world-writable directory. An attacker with local access to the device (without Administrator rights) can use symbolic links to trick the MSI installer into deleting files in locations that the attacker would otherwise have no access to. By creating a symlink from the world-writable directory to the target file, the attacker can manipulate the MSI installer's repair functionality to delete the target file during the repair process. Exploitation of this vulnerability could allow an attacker to delete important system files or replace them with malicious files, potentially leading to the affected device being compromised. The cloudflared client	ecurity/advisories/GHSA-7mjv-x3jf-545x	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			itself is not affected by this vulnerability, only the installer for 32-bit Windows devices. **CVE ID : CVE-2023-1314**		
Vendor: Cminds					
Product: cm_answers					
Affected Version(s): * Up to (including) 3.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeMindsSolutions CM Answers plugin <= 3.1.9 versions. **CVE ID : CVE-2023-25992**	N/A	A-CMI-CM_A-050423/548
Vendor: codemenschen					
Product: gift_vouchers					
Affected Version(s): * Up to (including) 4.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	The Gift Cards (Gift Vouchers and Packages) WordPress Plugin, version <= 4.3.1, is affected by an unauthenticated SQL injection vulnerability in the template parameter in the wpgv_doajax_voucher_pdf_save_func action. **CVE ID : CVE-2023-28662**	N/A	A-COD-GIFT-050423/549
Vendor: coder					
Product: code-server					
Affected Version(s): * Up to (excluding) 4.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	23-Mar-2023	9.3	Versions of the package code-server before 4.10.1 are vulnerable to Missing Origin Validation in WebSockets handshakes. Exploiting this vulnerability can allow an adversary in specific scenarios to access data from and connect to the code-server instance. **CVE ID : CVE-2023-26114**	https://github.com/coder/code-server/commit/d477972c68fc8c8e8d610aa7287db87ba90e55c7, https://security.snyk.io/vuln/SNYK-JS-CODESERVER-3368148	A-COD-CODE-050423/550
Vendor: collection.js_project					
Product: collection.js					
Affected Version(s): * Up to (excluding) 6.8.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	18-Mar-2023	7.5	Versions of the package collection.js before 6.8.1 are vulnerable to Prototype Pollution via the extend function in Collection.js/dist/node/iterators/extend.js. **CVE ID : CVE-2023-26113**	https://github.com/kobezzza/Collection/commit/d3d937645f62f37d3115d6aa90bb510fd856e6a2, https://github.com/kobezzza/Collection/issues/27, https://github.com/kobezzza/Collection/releases/tag/v6.8.1	A-COL-COLL-050423/551
Vendor: corebos					
Product: corebos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository tsolucio/corebos prior to 8.0. **CVE ID : CVE-2023-1527**	https://github.com/tsolucio/corebos/commit/aaaca69185bce2be6a82956c69541938dc871268, https://huntr.dev/bounties/f0272a31-9944-4545-8428-a26154d20348	A-COR-CORE-050423/552
Vendor: couchbase					
Product: couchbase_server					
Affected Version(s): From (including) 6.6.0 Up to (excluding) 7.1.4					
Missing Authentication for Critical Function	23-Mar-2023	5.3	In Couchbase Server 5 through 7 before 7.1.4, the nsstats endpoint is accessible without authentication. **CVE ID : CVE-2023-28470**	https://www.couchbase.com/alerts/, https://forums.couchbase.com/tags/security	A-COU-COUC-050423/553
Vendor: courtbouillon					
Product: cairosvg					
Affected Version(s): * Up to (excluding) 2.7.0					
Server-Side Request Forgery (SSRF)	20-Mar-2023	7.1	CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to version 2.7.0, Cairo can send requests to external hosts when processing SVG files. A	https://github.com/Kozea/CairoSVG/security/advisories/GHSA-rwmf-w63j-p7gv,	A-COU-CAIR-050423/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor could send a specially crafted SVG file that allows them to perform a server-side request forgery or denial of service. Version 2.7.0 disables CairoSVG's ability to access other files online by default. **CVE ID : CVE-2023-27586**	https://github.com/Kozea/CairoSVG/commit/12d31c653c0254fa9d9853f66b04ea46e7397255, https://github.com/Kozea/CairoSVG/commit/33007d4af9195e2bfb2ff9af064c4c2d8e4b2b53	
Vendor: crmeb					
Product: crmeb_java					
Affected Version(s): * Up to (including) 1.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been declared as critical. This vulnerability affects the function getAdminList of the file /api/admin/store/product/list. The manipulation of the argument cateId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223738 is the identifier assigned to this vulnerability.	N/A	A-CRM-CRME-050423/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1608		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been rated as problematic. This issue affects the function save of the file /api/admin/store/product/save. 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-223739. **CVE ID : CVE-2023-1609**	N/A	A-CRM-CRME-050423/556
Vendor: custom_content_shortcode_project					
Product: custom_content_shortcode					
Affected Version(s): * Up to (including) 4.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Mar-2023	8.8	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate one of its shortcode attribute, which could allow users with a contributor role and above to include arbitrary files via a traversal attack. This could also allow them to read non PHP files and retrieve their content. RCE could	N/A	A-CUS-CUST-050423/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also be achieved if the attacker manage to upload a malicious image containing PHP code, and then include it via the affected attribute, on a default WP install, authors could easily achieve that given that they have the upload_file capability. **CVE ID : CVE-2023-0340**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0273**	N/A	A-CUS-CUST-050423/558
Vendor: databasir					
Product: databasir					
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an Expression	28-Mar-2023	9.8	Databasir v1.0.7 was discovered to contain a remote code execution (RCE) vulnerability via the	N/A	A-DAT-DATA-050423/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Language Statement ('Expression Language Injection')			mockDataScript parameter. **CVE ID : CVE-2023-27821**		
Vendor: dataease					
Product: dataease					
Affected Version(s): * Up to (excluding) 1.18.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Mar-2023	9.8	Dataease is an open source data visualization and analysis tool. The blacklist for SQL injection protection is missing entries. This vulnerability has been fixed in version 1.18.5. There are no known workarounds. **CVE ID : CVE-2023-28437**	https://github.com/dataease/dataease/issues/4795, https://github.com/dataease/dataease/security/advisories/GHSA-7j7j-9rw6-3r56	A-DAT-DATA-050423/560
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	6.1	Dataease is an open source data visualization and analysis tool. The permissions for the file upload interface is not checked so users who are not logged in can upload directly to the background. The file type also goes unchecked, users could upload any type of file. These vulnerabilities has been fixed in version 1.18.5. **CVE ID : CVE-2023-28435**	https://github.com/dataease/dataease/security/advisories/GHSA-625h-q3g9-rffc	A-DAT-DATA-050423/561
Vendor: datagear					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: datagear					
Affected Version(s): * Up to (excluding) 1.12.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A vulnerability has been found in DataGear up to 1.11.1 and classified as problematic. This vulnerability affects unknown code of the component Plugin Handler. The manipulation leads to cross site scripting. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-223564. **CVE ID : CVE-2023-1572**	https://github.com/datageartech/datagear/releases/tag/v1.12.0	A-DAT-DATA-050423/562
Affected Version(s): * Up to (including) 1.11.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	A vulnerability was found in DataGear up to 1.11.1 and classified as problematic. This issue affects some unknown processing of the component Graph Dataset Handler. The manipulation leads to cross site scripting. The attack may be	N/A	A-DAT-DATA-050423/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-223565 was assigned to this vulnerability. **CVE ID : CVE-2023-1573**		
Affected Version(s): * Up to (including) 4.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in DataGear up to 4.5.0. This affects an unknown part of the file /analysisProject/pagingQueryData. The manipulation of the argument queryOrder leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.5.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-223563.	N/A	A-DAT-DATA-050423/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1571		
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): * Up to (including) 5.7.106					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dede/group_store.php endpoint. **CVE ID : CVE-2023-27707**	N/A	A-DED-DEDE-050423/565
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dedestory_catalog.php endpoint. **CVE ID : CVE-2023-27709**	N/A	A-DED-DEDE-050423/566
Vendor: deltaww					
Product: infrasuite_device_master					
Affected Version(s): * Up to (excluding) 1.0.5					
Deserialization of Untrusted Data	27-Mar-2023	9.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which the Device-status service listens on port 10100/ UDP by	N/A	A-DEL-INFR-050423/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default. The service accepts the unverified UDP packets and deserializes the content, which could allow an unauthenticated attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-1133**		
Missing Authentication for Critical Function	27-Mar-2023	9.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability that could allow an attacker to achieve unauthenticated remote code execution in the context of an administrator. **CVE ID : CVE-2023-1140**	N/A	A-DEL-INFR-050423/568
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	9.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use URL decoding to retrieve system files, credentials, and bypass authentication resulting in privilege escalation. **CVE ID : CVE-2023-1142**	N/A	A-DEL-INFR-050423/569
Improper Limitation of a Pathname	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by	N/A	A-DEL-INFR-050423/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			a path traversal vulnerability, which could allow an attacker to read local files, disclose plaintext credentials, and escalate privileges. **CVE ID : CVE-2023-1134**		
Insufficiently Protected Credentials	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which a low-level user could extract files and plaintext credentials of administrator users, resulting in privilege escalation. **CVE ID : CVE-2023-1137**	N/A	A-DEL-INFR-050423/571
Deserialization of Untrusted Data	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-gateway service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. **CVE ID : CVE-2023-1139**	N/A	A-DEL-INFR-050423/572
Improper Neutralization of Special Elements	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a command injection	N/A	A-DEL-INFR-050423/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			vulnerability that could allow an attacker to inject arbitrary commands, which could result in remote code execution. **CVE ID : CVE-2023-1141**		
N/A	27-Mar-2023	8.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use Lua scripts, which could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2023-1143**	N/A	A-DEL-INFR-050423/574
Incorrect Authorization	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contains an improper access control vulnerability in which an attacker can use the Device-Gateway service and bypass authorization, which could result in privilege escalation. **CVE ID : CVE-2023-1144**	N/A	A-DEL-INFR-050423/575
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	7.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could set incorrect directory permissions, which could result in	N/A	A-DEL-INFR-050423/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local privilege escalation. **CVE ID : CVE-2023-1135**		
Deserialization of Untrusted Data	27-Mar-2023	7.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-DataCollect service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. **CVE ID : CVE-2023-1145**	N/A	A-DEL-INFR-050423/577
Incorrect Authorization	27-Mar-2023	7.5	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an unauthenticated attacker could generate a valid token, which would lead to authentication bypass. **CVE ID : CVE-2023-1136**	N/A	A-DEL-INFR-050423/578
N/A	27-Mar-2023	7.5	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain an improper access control vulnerability, which could allow an attacker to retrieve Gateway configuration files to obtain plaintext credentials.	N/A	A-DEL-INFR-050423/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1138		
Vendor: deno					
Product: deno					
Affected Version(s): * Up to (excluding) 1.31.2					
Improper Neutralization of Escape, Meta, or Control Sequences	24-Mar-2023	8.8	Deno is a simple, modern and secure runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Arbitrary program names without any ANSI filtering allows any malicious program to clear the first 2 lines of a `op_spawn_child` or `op_kill` prompt and replace it with any desired text. This works with any command on the respective platform, giving the program the full ability to choose what program they wanted to run. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). This issue has been patched in version 1.31.2. **CVE ID : CVE-2023-28446**	https://github.com/denoland/deno/blob/7d13d65468c37022f003bb680dfbddd07ea72173/runtime/js/40_process.js#L175, https://github.com/denoland/deno/releases/tag/v1.31.2, https://github.com/denoland/deno/security/advisories/GHSA-vq67-rp93-65qf	A-DEN-DENO-050423/580
Affected Version(s): 1.32.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Mar-2023	9.8	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers. **CVE ID : CVE-2023-28445**	https://github.com/denoland/deno/pull/18395, https://github.com/denoland/deno/releases/tag/v1.32.1, https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx	A-DEN-DENO-050423/581
Product: deno_runtime					
Affected Version(s): 0.102.0					
Out-of-bounds Read	24-Mar-2023	9.8	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed	https://github.com/denoland/deno/pull/18395, https://git	A-DEN-DENO-050423/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers. **CVE ID : CVE-2023-28445**	hub.com/denoland/deno/releases/tag/v1.32.1, https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx	
Product: serde_v8					
Affected Version(s): 0.87.0					
Out-of-bounds Read	24-Mar-2023	9.8	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound	https://github.com/denoland/deno/pull/18395, https://github.com/denoland/deno/releases/tag/v1.32.1, https://git	A-DEN-SERD-050423/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers. **CVE ID : CVE-2023-28445**	hub.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx	
Vendor: Dino					
Product: dino					
Affected Version(s): * Up to (excluding) 0.2.3					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	A-DIN-DINO-050423/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 0.3.0 Up to (excluding) 0.3.2					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	A-DIN-DINO-050423/585
Affected Version(s): From (including) 0.4.0 Up to (excluding) 0.4.2					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	A-DIN-DINO-050423/586
Vendor: discourse					
Product: discourse					
Affected Version(s): 1.1.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the	https://github.com/discourse/discourse/pull	A-DIS-DISC-050423/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and	https://github.com/discourse/discourse/commit/f31f0	A-DIS-DISC-050423/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 1.2.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-`	https://github.com/discourse/discourse/pull/20004, https://github.com/di	A-DIS-DISC-050423/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	scourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed`	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f5744	A-DIS-DISC-050423/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	0452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 3.0.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105f	A-DIS-DISC-050423/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	ee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/di	A-DIS-DISC-050423/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	scourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): * Up to (excluding) 3.0.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9	A-DIS-DISC-050423/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
Affected Version(s): * Up to (excluding) 3.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included in a user's full name field to to carry out cross-site scripting	https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915, https://github.com/discourse/discourse/sec	A-DIS-DISC-050423/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse. **CVE ID : CVE-2023-25172**	urity/advisories/GHSA-7pm2-prxw-wrvp, https://github.com/discourse/discourse/pull/20008	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): * Up to (excluding) 3.1.0					
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched	https://github.com/discourse/discourse/pull/20710, https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh, https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c	A-DIS-DISC-050423/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28112**		
Server-Side Request Forgery (SSRF)	17-Mar-2023	7.5	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's server-side request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of Discourse. version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28111**	https://github.com/discourse/discourse/pull/20710, https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc, https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a	A-DIS-DISC-050423/597
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included	https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915, https://git	A-DIS-DISC-050423/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a user's full name field to to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse. **CVE ID : CVE-2023-25172**	hub.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp, https://github.com/discourse/discourse/pull/20008	
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is	https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61, https://github.com/discourse/discourse/pull/20700, https://github.com/discourse/discourse/security/advis	A-DIS-DISC-050423/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28107**	ories/GHSA-cp7c-fm4c-6xxx	
Affected Version(s): * Up to (including) 3.0.1					
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28107**	https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61, https://github.com/discourse/discourse/pull/20700, https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx	A-DIS-DISC-050423/600
Affected Version(s): * Up to (including) 3.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28112**	https://github.com/discourse/discourse/pull/20710, https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh, https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c	A-DIS-DISC-050423/601
Affected Version(s): 1.3.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105f	A-DIS-DISC-050423/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	ee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/di	A-DIS-DISC-050423/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	scourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 1.4.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9	A-DIS-DISC-050423/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advis	A-DIS-DISC-050423/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	ories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 1.5.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/di	A-DIS-DISC-050423/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	scourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 1.6.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9	A-DIS-DISC-050423/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 1.7.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f	A-DIS-DISC-050423/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 1.8.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 1.9.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 2.0.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 2.1.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**		
Affected Version(s): 2.2.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23935		
Affected Version(s): 2.3.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23622		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/623
Affected Version(s): 2.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	A-DIS-DISC-050423/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	A-DIS-DISC-050423/625
Affected Version(s): 2.5.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion	https://github.com/di	A-DIS-DISC-050423/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	scourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions	https://github.com/discourse/dis	A-DIS-DISC-050423/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	course/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 2.6.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and	https://github.com/discourse/discourse/pull/20004,	A-DIS-DISC-050423/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2	https://github.com/discourse/discourse/commit/f31f0b70f82c43	A-DIS-DISC-050423/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 2.7.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/dis	A-DIS-DISC-050423/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	course/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37,	A-DIS-DISC-050423/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 2.8.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b	A-DIS-DISC-050423/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	0ec23ff814a09d1c0c9ace95164, https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/dis	A-DIS-DISC-050423/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	course/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 2.9.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted	https://github.com/discourse/discourse/pull/20004, https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164,	A-DIS-DISC-050423/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions. **CVE ID : CVE-2023-23622**	https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f	
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA	A-DIS-DISC-050423/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	-rf8j-mf8c-82v7	
Affected Version(s): 3.1.0					
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse	https://github.com/discourse/discourse/pull/20710, https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh, https://github.com/discourse/discourse/co	A-DIS-DISC-050423/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28112**	mmit/39c2f63b35d90ebaf67b9604cf1d424e5984203c	
Server-Side Request Forgery (SSRF)	17-Mar-2023	7.5	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's server-side request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of Discourse. version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28111**	https://github.com/discourse/discourse/pull/20710, https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc, https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a	A-DIS-DISC-050423/637
Improper Neutralization of	17-Mar-2023	6.1	Discourse is an open-source discussion platform. Between	https://github.com/discourse/dis	A-DIS-DISC-050423/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			versions 3.1.0.beta2 and 3.1.0.beta3 of the `tests-passed` branch, editing or responding to a chat message containing malicious content could lead to a cross-site scripting attack. This issue is patched in version 3.1.0.beta3 of the `tests-passed` branch. There are no known workarounds. **CVE ID : CVE-2023-26040**	course/commit/a373bf2a01488c206e7feb28a9d2361b22ce6e70, https://github.com/discourse/discourse/security/advisories/GHSA-ccfc-qpmp-gq87	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included in a user's full name field to to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a	https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915, https://github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp, https://github.com/discourse/discourse/pull/20008	A-DIS-DISC-050423/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround, enable and/or restore your site's CSP to the default one provided with Discourse. **CVE ID : CVE-2023-25172**		
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. **CVE ID : CVE-2023-28107**	https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61, https://github.com/discourse/discourse/pull/20700, https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx	A-DIS-DISC-050423/640
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta`	https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6	A-DIS-DISC-050423/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting. **CVE ID : CVE-2023-23935**	fc0d4f57440452f37, https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Vendor: dreamer_cms_project					
Product: dreamer_cms					
Affected Version(s): 4.0.1					
Incorrect Permission Assignment for Critical Resource	16-Mar-2023	5.3	Permissions vulnerability found in isoftforce Dreamer CMS v.4.0.1 allows local attackers to obtain sensitive	N/A	A-DRE-DREA-050423/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information via the AttachmentController parameter. **CVE ID : CVE-2023-27084**		
Vendor: e-commerce_system_project					
Product: e-commerce_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester E-Commerce System 1.0. This issue affects some unknown processing of the file /ecommerce/admin/settings/setDiscount.php. The manipulation of the argument id with the input 201737 AND (SELECT 8973 FROM (SELECT(SLEEP(5)))OoAD) 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-223409 was assigned to this vulnerability. **CVE ID : CVE-2023-1505**	N/A	A-E-C-E-CO-050423/643
Improper Neutralization of Special Elements	20-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester E-Commerce System 1.0.	N/A	A-E-C-E-CO-050423/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Affected is an unknown function of the file login.php. The manipulation of the argument U_USERNAME 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-223410 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1506**		
Improper Access Control	22-Mar-2023	9.8	A vulnerability was found in SourceCodester E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ecommerce/admin/user/controller.php?action=edit of the component Username Handler. The manipulation of the argument USERID leads to improper access controls. The attack may be launched remotely. VDB-223550 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1557**	N/A	A-E-C-E-CO-050423/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	A vulnerability has been found in SourceCodester E-Commerce System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /ecommerce/admin/category/controller.php of the component Category Name Handler. The manipulation of the argument CATEGORY leads to cross site scripting. 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-223411. **CVE ID : CVE-2023-1507**	N/A	A-E-C-E-CO-050423/646
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A vulnerability classified as problematic was found in SourceCodester E-Commerce System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/user/controller.php?action=edit. The manipulation of the argument U_NAME with the input	N/A	A-E-C-E-CO-050423/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<script>alert('1')</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223561 was assigned to this vulnerability. **CVE ID : CVE-2023-1569**		
Vendor: e-dynamics					
Product: events_made_easy					
Affected Version(s): * Up to (including) 2.3.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The Events Made Easy WordPress Plugin, version <= 2.3.14 is affected by an authenticated SQL injection vulnerability in the 'search_name' parameter in the eme_recurrences_list action. **CVE ID : CVE-2023-28660**	N/A	A-E-D-EVEN-050423/648
Vendor: earnings_and_expense_tracker_application_project					
Product: earnings_and_expense_tracker_application					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Earnings and Expense Tracker App 1.0. This affects an unknown part of the file Master.php?a=save_ex	N/A	A-EAR-EARN-050423/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pense. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-224307. **CVE ID : CVE-2023-1688**		
Vendor: earnings_and_expense_tracker_app_project					
Product: earnings_and_expense_tracker_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	A vulnerability classified as problematic was found in SourceCodester Earnings and Expense Tracker App 1.0. This vulnerability affects unknown code of the file Master.php?a=save_earning. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-224308. **CVE ID : CVE-2023-1689**	N/A	A-EAR-EARN-050423/650
Vendor: ellucian					
Product: banner_web_tailor					
Affected Version(s): 8.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Mar-2023	8.8	** DISPUTED ** A vulnerability has been found in Ellucian Banner Web Tailor 8.6 and classified as critical. This vulnerability affects unknown code of the file /PROD_ar/twbkwbis.P_FirstMenu of the component Login Page. The manipulation of the argument PIDM/WEBID leads to improper authorization. The attack can be initiated remotely. After submitting proper login credentials it becomes possible to generate new valid session identifiers on the OTP page. The real existence of this vulnerability is still doubted at the moment. VDB-224014 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1632**	N/A	A-ELL-BANN-050423/651
Vendor: evilmartians					
Product: imgproxy					
Affected Version(s): * Up to (excluding) 3.14.0					
Improper Neutralization of Input	19-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository	https://huntr.dev/bounties/de603972-	A-EVI-IMGP-050423/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			imgproxy/imgproxy prior to 3.14.0. **CVE ID : CVE-2023-1496**	935a-401a-96fb-17ddadd282b2, https://github.com/imgproxy/imgproxy/commit/62f8d08a93d301285dcd1dabcc7ba10c6c65b689	
Vendor: evolucare					
Product: ecs_imaging					
Affected Version(s): 6.21.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** EVOLUCARE ECSIMAGING (aka ECS Imaging) < 6.21.5 is vulnerable to Cross Site Scripting (XSS) via new_movie. php. **CVE ID : CVE-2023-26913**	N/A	A-EVO-ECS_-050423/653
Vendor: Extplorer					
Product: extplorer					
Affected Version(s): 2.1.15					
N/A	21-Mar-2023	8.8	Insecure Permissions vulnerability found in Extplorer File manager eXtplorer v.2.1.15 allows a remote attacker to execute arbitrary code via the index.php compenent	N/A	A-EXT-EXTP-050423/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27842		
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Affected Version(s): 8.0					
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	A-FED-EXTR-050423/655
Affected Version(s): 9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	A-FED-EXTR-050423/656
Vendor: feifeicms					
Product: feifeicms					
Affected Version(s): 2.7.130201					
Improper Neutralization of Input During	22-Mar-2023	5.4	A vulnerability was found in FeiFeiCMS 2.7.130201. It has been classified as problematic. This	N/A	A-FEI-FEIF-050423/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			affects an unknown part of the file \Public\system\slide_add.html of the component Extension Tool. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223557 was assigned to this vulnerability. **CVE ID : CVE-2023-1565**		
Vendor: file_management_system_project					
Product: file_management_system					
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in File Management Project 1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field under the Edit User module. **CVE ID : CVE-2023-27245**	https://github.com/flyasolo/File-Management-System	A-FIL-FILE-050423/658
Vendor: Filseclab					
Product: twister_antivirus					
Affected Version(s): 8.0					
Improper Resource Shutdown or Release	17-Mar-2023	7.5	A vulnerability was found in Filseclab Twister Antivirus 8. It has been declared as problematic. This	N/A	A-FIL-TWIS-050423/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects the function 0x80112053 in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. 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-223288. **CVE ID : CVE-2023-1443**		
NULL Pointer Dereference	17-Mar-2023	6.5	A vulnerability was found in Filseclab Twister Antivirus 8. It has been rated as critical. This issue affects the function 0x8011206B in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223289 was assigned to this vulnerability. **CVE ID : CVE-2023-1444**	N/A	A-FIL-TWIS-050423/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability classified as problematic has been found in Filseclab Twister Antivirus 8. Affected is the function 0x80112053 in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-223290 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1445**	N/A	A-FIL-TWIS-050423/661
Vendor: fit2cloud					
Product: jumpserver					
Affected Version(s): * Up to (excluding) 2.28.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Mar-2023	9.9	Jumpserver is a popular open source bastion host, and Koko is a Jumpserver component that is the Go version of coco, refactoring coco's SSH/SFTP service and Web Terminal service. Prior to version 2.28.8, using illegal tokens to connect to a Kubernetes cluster through Koko can result in the execution	https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29, https://github.com/jumpserver/jumpserver/releases/tag/v2.28.8	A-FIT-JUMP-050423/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of dangerous commands that may disrupt the Koko container environment and affect normal usage. The vulnerability has been fixed in v2.28.8. **CVE ID : CVE-2023-28110**		
Product: koko					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Mar-2023	9.9	Jumpserver is a popular open source bastion host, and Koko is a Jumpserver component that is the Go version of coco, refactoring coco's SSH/SFTP service and Web Terminal service. Prior to version 2.28.8, using illegal tokens to connect to a Kubernetes cluster through Koko can result in the execution of dangerous commands that may disrupt the Koko container environment and affect normal usage. The vulnerability has been fixed in v2.28.8. **CVE ID : CVE-2023-28110**	https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29, https://github.com/jumpserver/jumpserver/releases/tag/v2.28.8	A-FIT-KOKO-050423/663
Vendor: Flatpak					
Product: Flatpak					
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust. **CVE ID : CVE-2023-28101**	https://github.com/flatpak/flatpak/commit/6cac99dafe6003c8a4bd56663416787536869, https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c, https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c	A-FLA-FLAT-050423/664
N/A	16-Mar-2023	10	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar	https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp, https://git	A-FLA-FLAT-050423/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment. **CVE ID : CVE-2023-28100**	hub.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9	
Affected Version(s): * Up to (excluding) 1.10.8					
Improper Encoding or	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running	https://github.com/flatpak/flatp	A-FLA-FLAT-050423/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust. **CVE ID : CVE-2023-28101**	ak/commit/6cac99dafe6003c8a4bd5666341c217876536869, https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c, https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c	
N/A	16-Mar-2023	10	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl	https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp, https://github.com/flatpak/flatpak/commit	A-FLA-FLAT-050423/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment. **CVE ID : CVE-2023-28100**	/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9	
Affected Version(s): From (including) 1.14.0 Up to (excluding) 1.14.4					
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to	https://github.com/flatpak/flatpak/commit/6cac99dafe6003c8a4	A-FLA-FLAT-050423/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust. **CVE ID : CVE-2023-28101**	bd5666341c217876536869, https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c, https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c	
N/A	16-Mar-2023	10	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux	https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp, https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8c	A-FLA-FLAT-050423/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment. **CVE ID : CVE-2023-28100**	a9ed73ed53be9	
Affected Version(s): From (including) 1.15.0 Up to (excluding) 1.15.4					
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a	https://github.com/flatpak/flatpak/commit/6cac99dafe6003c8a4bd5666341c217876536869,	A-FLA-FLAT-050423/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust. **CVE ID : CVE-2023-28101**	https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c, https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c	
N/A	16-Mar-2023	10	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the	https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp, https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9	A-FLA-FLAT-050423/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment. **CVE ID : CVE-2023-28100**		
Vendor: formidablepro2pdf					
Product: formidable_pro2pdf					
Affected Version(s): * Up to (excluding) 3.11					
Improper Neutralization of Special Elements used in an SQL Command	22-Mar-2023	8.8	The Formidable PRO2PDF WordPress Plugin, version < 3.11, is affected by an authenticated SQL injection vulnerability in the 'fieldmap' parameter in the	N/A	A-FOR-FORM-050423/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			fpropdf_export_file action. **CVE ID : CVE-2023-28663**		
Vendor: gadget_works_online_ordering_system_project					
Product: gadget_works_online_ordering_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	16-Mar-2023	7.2	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file admin/products/controller.php?action=add of the component Products Handler. The manipulation of the argument filename leads to unrestricted upload. 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-223215. **CVE ID : CVE-2023-1433**	https://github.com/zhengjiashengbaba/bug_report/blob/main/UPLOAD.md	A-GAD-GADG-050423/673
Vendor: galaxyproject					
Product: galaxy					
Affected Version(s): * Up to (excluding) 22.01					
Incorrect Authorization	20-Mar-2023	7.5	Galaxy is an open-source platform for data analysis. All supported versions of	https://github.com/galaxyproject/galaxy/se	A-GAL-GALA-050423/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Galaxy are affected prior to 22.01, 22.05, and 23.0 are affected by an insufficient permission check. Unsupported versions are likely affected as far back as the functionality of Visualizations/Pages exists. Due to this issue, an attacker can modify or delete any Galaxy Visualization or Galaxy Page given they know the encoded ID of it. Additionally, they can copy or import any Galaxy Visualization given they know the encoded ID of it. Patches are available for versions 22.01, 22.05, and 23.0. For the changes to take effect, you must restart all Galaxy server processes. There are no supported workarounds. **CVE ID : CVE-2023-27578**	curity/advisories/GHSA-j8q2-r4g5-f22j	
Vendor: GE					
Product: ifix					
Affected Version(s): 2022					
Improper Control of Generation of Code	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to	N/A	A-GE-IFIX-050423/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software. **CVE ID : CVE-2023-0598**		
Affected Version(s): 6.1					
Improper Control of Generation of Code ('Code Injection')	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software. **CVE ID : CVE-2023-0598**	N/A	A-GE-IFIX-050423/676
Affected Version(s): 6.5					
Improper Control of Generation of Code ('Code Injection')	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software.	N/A	A-GE-IFIX-050423/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0598		
Vendor: generalbytes					
Product: crypto_application_server					
Affected Version(s): 20230120					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.1	General Bytes Crypto Application Server (CAS) 20230120, as distributed with General Bytes BATM devices, allows remote attackers to execute arbitrary Java code by uploading a Java application to the /batm/app/admin/standalone/deployments directory, aka BATM-4780, as exploited in the wild in March 2023. This is fixed in 20221118.48 and 20230120.44. **CVE ID : CVE-2023-28725**	https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2885222430/Security+Incident+March+17-18th+2023	A-GEN-CRYP-050423/678
Vendor: Gentoo					
Product: soko					
Affected Version(s): * Up to (excluding) 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q`	https://gitweb.gentoo.org/sites/soko.git/commit/?id=4fa6e4b619c0362728955b6ec56eab0e0cbf1e23, https://github.com/gentoo/soko	A-GEN-SOKO-050423/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on `https://packages.gentoo.org/`. It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit `4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y` of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries. **CVE ID : CVE-2023-28424**	/security/advisories/GHSA-gc2x-86p3-mxg2	
Vendor: geosolutionsgroup					
Product: geonode					
Affected Version(s): * Up to (excluding) 2.18.7					
Exposure of Sensitive Information to an Unauthorized Actor	24-Mar-2023	5.3	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the `/geoserver/rest/abo	https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w, https://github.com/GeoNode/geoserver-geonode-ext/blob/2.	A-GEO-GEON-050423/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ut/status` Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the	20.7/data/security/rest.properties	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing `<geoserver_datadir>/security/rest.properties` file. **CVE ID : CVE-2023-28442**		
Affected Version(s): From (including) 2.19.0 Up to (excluding) 2.19.6					
Exposure of Sensitive Information to an Unauthorized Actor	24-Mar-2023	5.3	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the `/geoserver/rest/about/status` Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration	https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w, https://github.com/GeoNode/geoserver-geonode-ext/blob/2.20.7/data/security/rest.properties	A-GEO-GEON-050423/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing `<geoserver_datadir>/security/rest.properties` file. **CVE ID : CVE-2023-28442**		
Affected Version(s): From (including) 2.20.0 Up to (excluding) 2.20.6					
Exposure of Sensitive Informatio	24-Mar-2023	5.3	GeoNode is an open source platform that facilitates the creation,	https://github.com/GeoNode/ge	A-GEO-GEON-050423/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the `/geoserver/rest/about/status` Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has	onode/security/advisories/GHSA-87mh-vw7c-5v6w, https://github.com/GeoNode/geoserver-geonode-ext/blob/2.20.7/data/security/rest.properties	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing `<geoserver_datadir>/security/rest.properties` file. **CVE ID : CVE-2023-28442**		
Vendor: getresponse					
Product: getresponse					
Affected Version(s): * Up to (excluding) 5.5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The GetResponse for WordPress plugin through 5.5.31 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-GET-GETR-050423/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0167		
Vendor: getshortcodes					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (excluding) 5.12.8					
Missing Authorization	20-Mar-2023	6.5	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not ensure that posts to be displayed via some shortcodes are already public and can be accessed by the user making the request, allowing any authenticated users such as subscriber to view draft, private or even password protected posts. It is also possible to leak the password of protected posts **CVE ID : CVE-2023-0890**	N/A	A-GET-SHOR-050423/684
Missing Authorization	20-Mar-2023	6.5	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not validate the user meta to be retrieved via the user shortcode, allowing any authenticated users such as subscriber to retrieve arbitrary user meta (except the user_pass), such as the user email and	N/A	A-GET-SHOR-050423/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activation key by default. **CVE ID : CVE-2023-0911**		
Vendor: gmace_project					
Product: gmace					
Affected Version(s): * Up to (including) 1.5.2					
Cross-Site Request Forgery (CSRF)	29-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in German Mesky GMAce plugin <= 1.5.2 versions. **CVE ID : CVE-2023-23861**	N/A	A-GMA-GMAC-050423/686
Vendor: GNU					
Product: org_mode					
Affected Version(s): * Up to (including) 9.6.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Mar-2023	7.8	org-babel-execute:latex in ob-latex.el in Org Mode through 9.6.1 for GNU Emacs allows attackers to execute arbitrary commands via a file name or directory name that contains shell metacharacters. **CVE ID : CVE-2023-28617**	https://list.orgmode.org/tencent_04CF842704737012CCBCD63CD654DD41CA0A@qq.com/T/#m6ef8e7d34b25fe17b4cbb655b161edce18c6655e, https://git.savannah.gnu.org/cgit/emacs/org-mode.git/commit/?id=8f8ec2ccf3f5ef8f38d	A-GNU-ORG_-050423/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				68ec84a7e4739c45db485	
Vendor: go-huge-util_project					
Product: go-huge-util					
Affected Version(s): * Up to (excluding) 0.0.34					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	8.8	go-used-util has commonly used utility functions for Go. Versions prior to 0.0.34 have a ZipSlip issue when using fsutil package to unzip files. When users use `zip.Unzip` to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. The issue has been fixed in version 0.0.34. There are no known workarounds. **CVE ID : CVE-2023-28105**	https://github.com/dablelv/go-huge-util/commit/0e308b0fac8973e6fa251b0ab095cdc5c1c0956b	A-GO--GO-H-050423/688
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 111.0.5563.110					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Mar-2023	9.8	Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High)	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1529		
Use After Free	21-Mar-2023	8.8	Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1528**	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/690
Use After Free	21-Mar-2023	8.8	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1530**	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/691
Use After Free	21-Mar-2023	8.8	Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1531		
Out-of-bounds Read	21-Mar-2023	8.8	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1532**	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/693
Use After Free	21-Mar-2023	8.8	Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1533**	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/694
Use After Free	21-Mar-2023	8.8	Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-050423/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1534		
Product: tensorflow					
Affected Version(s): * Up to (excluding) 2.12.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Mar-2023	9.8	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAvgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. **CVE ID : CVE-2023-25664**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6hg6-5c2q-7rcr, https://github.com/tensorflow/tensorflow/commit/ddaac2bdd099bec5d7923dea45276a7558217e5b	A-GOO-TENS-050423/696
Out-of-bounds Read	25-Mar-2023	9.8	TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1.	https://github.com/tensorflow/tensorflow/commit/7b174a0f2e40ff3f3aa957aecddfd5aaae35eccb, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gw97-ff7c-9v96	A-GOO-TENS-050423/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25668		
Out-of-bounds Read	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, an out of bounds read is in GRUBlockCellGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. **CVE ID : CVE-2023-25658**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-68v3-g9cm-rmm6, https://github.com/tensorflow/tensorflow/commit/ff459137c2716a2a60f7d441b855fcb466d778cb	A-GOO-TENS-050423/698
Out-of-bounds Read	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the parameter `indices` for `DynamicStitch` does not match the shape of the parameter `data`, it can trigger an stack OOB read. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25659**	https://github.com/tensorflow/tensorflow/commit/ee004b18b976eeb5a758020af8880236cd707d05, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-93vr-9q9m-pj8p	A-GOO-TENS-050423/699
NULL Pointer	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions	https://github.com/tensorflow/tensorflow/	A-GOO-TENS-050423/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			2.12.0 and 2.11.1, when the parameter `summarize` of `tf.raw_ops.Print` is zero, the new method `SummarizeArray<bool>` will reference to a nullptr, leading to a seg fault. A fix is included in TensorFlow version 2.12 and version 2.11.1. **CVE ID : CVE-2023-25660**	commit/6d423b8bcc9aa9f5554dc988c1c16d038b508df1, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qjqc-vqcf-5qvj	
Integer Overflow or Wraparound	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 are vulnerable to integer overflow in EditDistance. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25662**	https://github.com/tensorflow/tensorflow/commit/08b8e18643d6dcde00890733b270ff8d9960c56c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7jvm-xxmr-v5cw	A-GOO-TENS-050423/701
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `ctx->step_containter()` is a null ptr, the Lookup function will be executed with a null	https://github.com/tensorflow/tensorflow/commit/239139d2ae6a81ae9ba499ad78b56d9b2931538a,	A-GOO-TENS-050423/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer. A fix is included in TensorFlow 2.12.0 and 2.11.1. **CVE ID : CVE-2023-25663**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-64jg-wjww-7c5w	
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `SparseSparseMaximum` is given invalid sparse tensors as inputs, it can give a null pointer error. A fix is included in TensorFlow version 2.12 and version 2.11.1. **CVE ID : CVE-2023-25665**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-558h-mq8x-7q9g, https://github.com/tensorflow/tensorflow/commit/5e0ecfb42f5f65629fd7a4edd6c4afe7ff0feb04	A-GOO-TENS-050423/703
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a floating point exception in AudioSpectrogram. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25666**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f637-vh3r-vfh2, https://github.com/tensorflow/tensorflow/commit/d0d4e779da0d0f56499c6fa5ba09f0	A-GOO-TENS-050423/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				a576cc6b14	
Integer Overflow or Wraparound	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, integer overflow occurs when `2^31 <= num_frames * height * width * channels < 2^32`, for example Full HD screencast of at least 346 frames. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25667**	https://github.com/tensorflow/tensorflow/commit/8dc723fcdd1a6127d6c970bd2ecb18b019a1a58d, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqm2-gh8w-gr68	A-GOO-TENS-050423/705
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the stride and window size are not positive for `tf.raw_ops.AvgPoolGrad`, it can give a floating point exception. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25669**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rcf8-g8jv-vg6p, https://github.com/tensorflow/tensorflow/commit/1295ae4dbb52fe06b19733b0257e2340d7b63b8d	A-GOO-TENS-050423/706
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to	https://github.com/tensorflow/tensorflow/	A-GOO-TENS-050423/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.12.0 and 2.11.1 have a null point error in QuantizedMatMulWithBiasAndDequantize with MKL enabled. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25670**	commit/8a47a39d9697969206d23a523c977238717e8727, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-49rq-hwc3-x77w	
Out-of-bounds Write	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. There is out-of-bounds access due to mismatched integer type sizes. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25671**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j5w9-hmfh-4cr6, https://github.com/tensorflow/tensorflow/commit/2eedc8f676d2c3b8be9492e547b2bc814c10b367	A-GOO-TENS-050423/708
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. The function `tf.raw_ops.LookupTableImportV2` cannot handle scalars in the `values` parameter and gives an NPE. A fix is included in TensorFlow version	https://github.com/tensorflow/tensorflow/commit/980b22536abcbbe1b4a5642fc940af33d8c19b69, https://	A-GOO-TENS-050423/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25672**	hub.com/tensorflow/tensorflow/security/advisories/GHSA-94mm-g2mv-8p7r	
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a Floating Point Exception in TensorListSplit with XLA. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. **CVE ID : CVE-2023-25673**	https://github.com/tensorflow/tensorflow/commit/728113a3be690facad6ce436660a0bc1858017fa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-647v-r7qq-24fh	A-GOO-TENS-050423/710
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source machine learning platform. Versions prior to 2.12.0 and 2.11.1 have a null pointer error in RandomShuffle with XLA enabled. A fix is included in TensorFlow 2.12.0 and 2.11.1. **CVE ID : CVE-2023-25674**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gf97-q72m-7579, https://github.com/tensorflow/tensorflow/commit/728113a3be690facad6ce436660a0b	A-GOO-TENS-050423/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c1858017fa	
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an end-to-end open source platform for machine learning. Constructing a tflite model with a paramater `filter_input_channel` of less than 1 gives a FPE. This issue has been patched in version 2.12. TensorFlow will also cherrypick the fix commit on TensorFlow 2.11.1. **CVE ID : CVE-2023-27579**	https://github.com/tensorflow/tensorflow/commit/34f8368c535253f5c9cb3a303297743b62442aaa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-5w96-866f-6rm8	A-GOO-TENS-050423/712
Vendor: gotowp					
Product: gotowp					
Affected Version(s): * Up to (including) 5.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The GoToWP WordPress plugin through 5.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0369**	N/A	A-GOT-GOTO-050423/713
Vendor: gpac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gpac					
Affected Version(s): * Up to (including) 2.2.0					
Uncontrolled Resource Consumption	27-Mar-2023	7.8	Denial of Service in GitHub repository gpac/gpac prior to 2.4.0. **CVE ID : CVE-2023-1654**	https://huntr.dev/bounties/33652b56-128f-41a7-afcc-10641f69ff14, https://github.com/gpac/gpac/commit/2c055153d401b8c49422971e3a0159869652d3da	A-GPA-GPAC-050423/714
Affected Version(s): 2.3					
Heap-based Buffer Overflow	17-Mar-2023	7.8	A vulnerability, which was classified as problematic, was found in GPAC 2.3-DEV-rev35-gbbca86917-master. This affects the function gf_m2ts_process_sdt of the file media_tools/mpegts.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier VDB-223293	N/A	A-GPA-GPAC-050423/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was assigned to this vulnerability. **CVE ID : CVE-2023-1448**		
Double Free	17-Mar-2023	7.8	A vulnerability has been found in GPAC 2.3-DEV-rev35-gbbca86917-master and classified as problematic. This vulnerability affects the function gf_av1_reset_state of the file media_tools/av_parsers.c. The manipulation leads to double free. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-223294 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1449**	https://github.com/gpac/gpac/issues/2387	A-GPA-GPAC-050423/716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Mar-2023	7.8	A vulnerability was found in GPAC 2.3-DEV-rev35-gbbca86917-master. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file filters/load_text.c. The manipulation leads to buffer overflow. Local	N/A	A-GPA-GPAC-050423/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access is required to approach this attack. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier VDB-223297 was assigned to this vulnerability. **CVE ID : CVE-2023-1452**		
Vendor: grafana					
Product: grafana					
Affected Version(s): From (excluding) 9.3.0 Up to (excluding) 9.3.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Grafana is an open-source platform for monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description.	https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76, https://grafana.com/security/security-advisories/cve-2023-1410/	A-GRA-GRAF-050423/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. **CVE ID : CVE-2023-1410**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Grafana is an open-source platform for monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. **CVE ID : CVE-2023-1410**	https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76, https://grafana.com/security/security-advisories/cve-2023-1410/	A-GRA-GRAF-050423/719
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.15					
Improper Neutralizat	23-Mar-2023	4.8	Grafana is an open-source platform for	https://github.com/gr	A-GRA-GRAF-050423/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. **CVE ID : CVE-2023-1410**	afana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76, https://grafana.com/security/security-advisories/cve-2023-1410/	
Vendor: greenshiftwp					
Product: greenshift_-_animation_and_page_builder_blocks					
Affected Version(s): * Up to (including) 4.9.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	Auth. (author+) Cross-Site Scripting (XSS) vulnerability in Wpsoul Greenshift – animation and page builder blocks plugin <= 4.9.9 versions. **CVE ID : CVE-2023-22707**	N/A	A-GRE-GREE-050423/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: hasthemes					
Product: contact_form_7_widget_for_elementor_page_builder_\&_gutenberg_blocks					
Affected Version(s): * Up to (excluding) 1.1.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Contact Form 7 Widget For Elementor Page Builder & Gutenberg Blocks WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0484**	N/A	A-HAS-CONT-050423/722
Product: coupon_zen					
Affected Version(s): * Up to (excluding) 1.0.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Coupon Zen WordPress plugin before 1.0.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-1089**	N/A	A-HAS-COUP-050423/723
Product: ever_compare					
Affected Version(s): * Up to (including) 1.2.3					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Ever Compare WordPress plugin through 1.2.3 does not have CSRF check when	N/A	A-HAS-EVER-050423/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0505**		
Product: free_woocommerce_theme_99fy_extension					
Affected Version(s): * Up to (excluding) 1.2.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Free WooCommerce Theme 99fy Extension WordPress plugin before 1.2.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0503**	N/A	A-HAS-FREE-050423/725
Product: ht_event					
Affected Version(s): * Up to (excluding) 1.4.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Event WordPress plugin before 1.4.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0496**	N/A	A-HAS-HT_E-050423/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ht_politic					
Affected Version(s): * Up to (excluding) 2.3.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Politic WordPress plugin before 2.3.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0504**	N/A	A-HAS-HT_P-050423/727
Product: ht_portfolio					
Affected Version(s): * Up to (excluding) 1.1.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Portfolio WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0497**	N/A	A-HAS-HT_P-050423/728
Product: ht_slider_for_elementor					
Affected Version(s): * Up to (excluding) 1.4.0					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Slider For Elementor WordPress plugin before 1.4.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate	N/A	A-HAS-HT_S-050423/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0495**		
Product: preview_link_generator					
Affected Version(s): * Up to (excluding) 1.0.4					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Preview Link Generator WordPress plugin before 1.0.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-1086**	N/A	A-HAS-PREV-050423/730
Product: quickswish					
Affected Version(s): * Up to (excluding) 1.1.0					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The QuickSwish WordPress plugin before 1.1.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0499**	N/A	A-HAS-QUIC-050423/731
Product: wc_sales_notification					
Affected Version(s): * Up to (excluding) 1.2.3					
Cross-Site Request	27-Mar-2023	4.3	The WC Sales Notification	N/A	A-HAS-WC_S-050423/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			WordPress plugin before 1.2.3 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-1087**		
Product: wp_education					
Affected Version(s): * Up to (excluding) 1.2.7					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The WP Education WordPress plugin before 1.2.7 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0498**	N/A	A-HAS-WP_E-050423/733
Product: wp_film_studio					
Affected Version(s): * Up to (excluding) 1.3.5					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP Film Studio WordPress plugin before 1.3.5 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack	N/A	A-HAS-WP_F-050423/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0500		
Product: wp_insurance					
Affected Version(s): * Up to (excluding) 2.1.4					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP Insurance WordPress plugin before 2.1.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0501**	N/A	A-HAS-WP_I-050423/735
Product: wp_news					
Affected Version(s): * Up to (including) 1.1.9					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP News WordPress plugin through 1.1.9 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-0502**	N/A	A-HAS-WP_N-050423/736
Product: wp_plugin_manager					
Affected Version(s): * Up to (excluding) 1.1.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The WP Plugin Manager WordPress plugin before 1.1.8 does not have CSRF check when activating plugins, which could	N/A	A-HAS-WP_P-050423/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack **CVE ID : CVE-2023-1088**		
Vendor: hgiga					
Product: oaklouds_mailsherlock					
Affected Version(s): 4.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	7.2	HGiga MailSherlock mail query function has vulnerability of insufficient validation for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject SQL commands to read, modify, and delete the database. **CVE ID : CVE-2023-24840**	https://www.twcert.org.tw/tw/cp-132-6959-cdecb-1.html	A-HGI-OAKL-050423/738
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	7.2	HGiga MailSherlock query function for connection log has a vulnerability of insufficient filtering for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system	https://www.twcert.org.tw/tw/cp-132-6960-fc2fe-1.html	A-HGI-OAKL-050423/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation or disrupt service. **CVE ID : CVE-2023-24841**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	HGiga MailSherlock's specific function has insufficient filtering for user input. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript, conducting a reflected XSS attack. **CVE ID : CVE-2023-24839**	https://www.twcert.org.tw/tw/cp-132-6958-e1a8e-1.html	A-HGI-OAKL-050423/740
Authorization Bypass Through User-Controlled Key	27-Mar-2023	5.3	HGiga MailSherlock has vulnerability of insufficient access control. An unauthenticated remote user can exploit this vulnerability to access partial content of another user's mail by changing user ID and mail ID within URL. **CVE ID : CVE-2023-24842**	https://www.twcert.org.tw/tw/cp-132-6961-12444-1.html	A-HGI-OAKL-050423/741
Product: oaklouds_portal					
Affected Version(s): From (including) 2.0 Up to (excluding) 2.0-10					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	9.8	HGiga OAKlouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to	https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html	A-HGI-OAKL-050423/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload and run arbitrary executable files to perform arbitrary command or disrupt service. **CVE ID : CVE-2023-25909**		
Affected Version(s): From (including) 3.0 Up to (excluding) 3.0-10					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	9.8	HGiga OAKlouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary command or disrupt service. **CVE ID : CVE-2023-25909**	https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html	A-HGI-OAKL-050423/743
Vendor: hkcms_project					
Product: hkcms					
Affected Version(s): 2.2.4.230206					
Improper Control of Generation of Code ('Code Injection')	18-Mar-2023	8.8	A vulnerability, which was classified as problematic, was found in HkCms 2.2.4.230206. This affects an unknown part of the file /admin.php/appcenter/local.html?type=addon of the component External Plugin Handler. The manipulation leads to code injection. It is	N/A	A-HKC-HKCM-050423/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223365 was assigned to this vulnerability. **CVE ID : CVE-2023-1482**		
Vendor: hu-manity					
Product: cookie_notice_\&_compliance_for_gdpr_\/_ccpa					
Affected Version(s): * Up to (excluding) 2.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Cookie Notice & Compliance for GDPR / CCPA WordPress plugin before 2.4.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0823**	N/A	A-HU--COOK-050423/745
Vendor: IBM					
Product: aspera_faspex					
Affected Version(s): * Up to (including) 4.4.2					
Improper Restriction of XML External	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote	https://www.ibm.com/support/pages/node/6964694, https://exc	A-IBM-ASPE-050423/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845. **CVE ID : CVE-2023-27874**	hange.xforce.ibmcloud.com/vulnerabilities/249845	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force ID: 249613. **CVE ID : CVE-2023-27871**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249613	A-IBM-ASPE-050423/747
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. **CVE ID : CVE-2023-27873**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249654	A-IBM-ASPE-050423/748
Affected Version(s): 4.4.2					
Improper Restriction of XML External Entity Reference	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulner	A-IBM-ASPE-050423/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. IBM X-Force ID: 249845. **CVE ID : CVE-2023-27874**	abilities/249845	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force ID: 249613. **CVE ID : CVE-2023-27871**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249613	A-IBM-ASPE-050423/750
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. **CVE ID : CVE-2023-27873**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249654	A-IBM-ASPE-050423/751
Affected Version(s): 5.0.4					
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. **CVE ID : CVE-2023-27875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249847, https://www.ibm.com/support/pages/node/6963662	A-IBM-ASPE-050423/752
Product: security_key_lifecycle_manager					
Affected Version(s): 3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. **CVE ID : CVE-2023-25684**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/753
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. **CVE ID : CVE-2023-25924**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247630	A-IBM-SECU-050423/754
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulner	A-IBM-SECU-050423/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorization. IBM X-Force ID: 247629. **CVE ID : CVE-2023-25923**	abilities/247629	
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. **CVE ID : CVE-2023-25686**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247601	A-IBM-SECU-050423/756
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606. **CVE ID : CVE-2023-25688**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247606	A-IBM-SECU-050423/757
Improper Limitation of a Pathname to a Restricted Directory	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.	A-IBM-SECU-050423/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. **CVE ID : CVE-2023-25689**	com/vulnerabilities/247618	
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. **CVE ID : CVE-2023-25687**	https://www.ibm.com/support/pages/node/6962729	A-IBM-SECU-050423/759
Affected Version(s): 3.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. **CVE ID : CVE-2023-25684**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. **CVE ID : CVE-2023-25924**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247630	A-IBM-SECU-050423/761
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. **CVE ID : CVE-2023-25923**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247629	A-IBM-SECU-050423/762
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. **CVE ID : CVE-2023-25686**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247601	A-IBM-SECU-050423/763
Improper Limitation	22-Mar-2023	5.3	IBM Security Guardium Key	https://www.ibm.com	A-IBM-SECU-050423/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606. **CVE ID : CVE-2023-25688**	/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247606	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. **CVE ID : CVE-2023-25689**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247618	A-IBM-SECU-050423/765
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log	https://www.ibm.com/support/pages/node/6962729	A-IBM-SECU-050423/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. IBM X-Force ID: 247602. **CVE ID : CVE-2023-25687**		
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. **CVE ID : CVE-2023-25684**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/767
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. **CVE ID : CVE-2023-25924**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247630	A-IBM-SECU-050423/768
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an	https://www.ibm.com/support/pages/node/6962729,	A-IBM-SECU-050423/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. **CVE ID : CVE-2023-25923**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247629	
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. **CVE ID : CVE-2023-25686**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247601	A-IBM-SECU-050423/770
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606. **CVE ID : CVE-2023-25688**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247606	A-IBM-SECU-050423/771
Improper Limitation of a	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0,	https://www.ibm.com/support/p	A-IBM-SECU-050423/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. **CVE ID : CVE-2023-25689**	ages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247618	
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. **CVE ID : CVE-2023-25687**	https://www.ibm.com/support/pages/node/6962729	A-IBM-SECU-050423/773
Affected Version(s): 4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 247597. **CVE ID : CVE-2023-25684**		
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. **CVE ID : CVE-2023-25924**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247630	A-IBM-SECU-050423/775
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. **CVE ID : CVE-2023-25923**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247629	A-IBM-SECU-050423/776
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601.	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulner	A-IBM-SECU-050423/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25686	abilities/247601	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606. **CVE ID : CVE-2023-25688**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247606	A-IBM-SECU-050423/778
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. **CVE ID : CVE-2023-25689**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247618	A-IBM-SECU-050423/779
Insertion of Sensitive Informatio	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and	https://www.ibm.com/support/p	A-IBM-SECU-050423/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. **CVE ID : CVE-2023-25687**	ages/node/6962729	
Affected Version(s): 4.1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. **CVE ID : CVE-2023-25684**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/781
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. **CVE ID : CVE-2023-25924**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247630	A-IBM-SECU-050423/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. **CVE ID : CVE-2023-25923**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247629	A-IBM-SECU-050423/783
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. **CVE ID : CVE-2023-25686**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247601	A-IBM-SECU-050423/784
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606.	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247606	A-IBM-SECU-050423/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25688		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. **CVE ID : CVE-2023-25689**	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247618	A-IBM-SECU-050423/786
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. **CVE ID : CVE-2023-25687**	https://www.ibm.com/support/pages/node/6962729	A-IBM-SECU-050423/787
Vendor: ibos					
Product: ibos					
Affected Version(s): 4.5.5					
Improper Neutralization of Special Elements used in an	18-Mar-2023	9.8	A vulnerability classified as critical has been found in IBOS 4.5.5. Affected is an unknown function of the file	N/A	A-IBO-IBOS-050423/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			ApiController.php. The manipulation of the argument emailids leads to sql injection. 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-223380. **CVE ID : CVE-2023-1494**		
Vendor: Imagemagick					
Product: imagemagick					
Affected Version(s): * Up to (excluding) 7.1.1-0					
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	A-IMA-IMAG-050423/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**		
Vendor: implecode					
Product: ecommerce_product_catalog					
Affected Version(s): * Up to (excluding) 3.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	4.8	The eCommerce Product Catalog plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, 3.3.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1470**	https://plugins.trac.wordpress.org/changeset/2881773/ecommerce-product-catalog/trunk/modules/price/price-settings.php	A-IMP-ECOM-050423/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: independentsoft					
Product: jodf					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JODF before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. **CVE ID : CVE-2023-28150**	N/A	A-IND-JODF-050423/791
Product: jspreadsheet					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JSpreadsheet before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. **CVE ID : CVE-2023-28151**	N/A	A-IND-JSPR-050423/792
Product: jword					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JWord before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. **CVE ID : CVE-2023-28152**	N/A	A-IND-JWOR-050423/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: invernyx					
Product: smartcars_3					
Affected Version(s): * Up to (excluding) 0.5.9					
Insertion of Sensitive Information into Log File	24-Mar-2023	7.5	smartCARS 3 is flight tracking software. In version 0.5.8 and prior, all persons who have failed login attempts will have their password stored in error logs. This problem doesn't occur in version 0.5.9. As a workaround, delete the affected log file, and ensure one logs in correctly. **CVE ID : CVE-2023-28441**	https://github.com/invernyx/smartcars-3-bugs/security/advisories/GHSA-fp42-c8g2-5jc7	A-INV-SMAR-050423/794
Vendor: Iobit					
Product: malware_fighter					
Affected Version(s): 9.4.0.776					
Out-of-bounds Write	26-Mar-2023	7.8	A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been declared as critical. This vulnerability affects the function 0x8018E000/0x8018E004 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be	N/A	A-IOB-MALW-050423/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-224026 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1646**		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been rated as problematic. Affected by this issue is the function 0x8001E024/0x8001E040 in the library ImfRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-224018 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1638**	N/A	A-IOB-MALW-050423/796
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability classified as problematic has been found in IObit Malware Fighter 9.4.0.776. This affects the function 0x8001E04C in the library ImfRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is	N/A	A-IOB-MALW-050423/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224019. **CVE ID : CVE-2023-1639**		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability classified as problematic was found in IObit Malware Fighter 9.4.0.776. This vulnerability affects the function 0x222010 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224020. **CVE ID : CVE-2023-1640**	N/A	A-IOB-MALW-050423/798
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in IObit Malware Fighter 9.4.0.776. This issue affects the function	N/A	A-IOB-MALW-050423/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x222018 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224021 was assigned to this vulnerability. **CVE ID : CVE-2023-1641**		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability, which was classified as problematic, was found in IObit Malware Fighter 9.4.0.776. Affected is the function 0x222034/0x222038/0x22203C/0x222040 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-224022 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1642**	N/A	A-IOB-MALW-050423/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability has been found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this vulnerability is the function 0x8001E000/0x8001E004/0x8001E018/0x8001E01C/0x8001E024/0x8001E040 in the library ImfHpRegFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224023. **CVE ID : CVE-2023-1643**	N/A	A-IOB-MALW-050423/801
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability was found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this issue is the function 0x8018E010 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is possible to launch the	N/A	A-IOB-MALW-050423/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224024. **CVE ID : CVE-2023-1644**		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been classified as problematic. This affects the function 0x8018E008 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224025 was assigned to this vulnerability. **CVE ID : CVE-2023-1645**	N/A	A-IOB-MALW-050423/803
Vendor: isdecisions					
Product: userlock					
Affected Version(s): 11.0.1					
Incorrect Authorization	23-Mar-2023	7.2	IS Decisions UserLock MFA 11.01 is vulnerable to authentication bypass using scheduled task.	N/A	A-ISD-USER-050423/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23192		
Vendor: jc21					
Product: nginx_proxy_manager					
Affected Version(s): 2.9.19					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-2023	9.8	An issue found in NginxProxyManager v.2.9.19 allows an attacker to execute arbitrary code via a lua script to the configuration file. **CVE ID : CVE-2023-27224**	N/A	A-JC2-NGIN-050423/805
Vendor: jeecg					
Product: jeecg-boot					
Affected Version(s): 3.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical has been found in jeecg-boot 3.5.0. This affects an unknown part of the file jmreport/qurestSql. The manipulation of the argument apiSelectId 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-223299. **CVE ID : CVE-2023-1454**	N/A	A-JEE-JEEC-050423/806
Vendor: Jenkins					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: absint_a3					
Affected Version(s): * Up to (including) 1.1.0					
Improper Restriction of XML External Entity Reference	22-Mar-2023	7.1	Jenkins AbsInt a^3 Plugin 1.1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2023-28685**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2930	A-JEN-ABSI-050423/807
Vendor: jettison_project					
Product: jettison					
Affected Version(s): * Up to (excluding) 1.5.4					
Uncontrolled Recursion	22-Mar-2023	7.5	An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown. **CVE ID : CVE-2023-1436**	N/A	A-JET-JETT-050423/808
Vendor: Jiangmin					
Product: jiangmin_antivirus					
Affected Version(s): 16.2.2022.418					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Mar-2023	7.8	A vulnerability classified as critical was found in JiangMin Antivirus 16.2.2022.418. Affected by this vulnerability is the function 0x222010 in the library kvcore.sys of the component	N/A	A-JIA-JIAN-050423/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL Handler. The manipulation leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224011. **CVE ID : CVE-2023-1629**		
NULL Pointer Dereference	25-Mar-2023	5.5	A vulnerability classified as problematic has been found in Jianming Antivirus 16.2.2022.418. Affected is an unknown function in the library kvcore.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-224010 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1628**	N/A	A-JIA-JIAN-050423/810
Improper Resource Shutdown or Release	25-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in JiangMin Antivirus	N/A	A-JIA-JIAN-050423/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.2.2022.418. Affected by this issue is the function 0x222000 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224012. **CVE ID : CVE-2023-1630**		
NULL Pointer Dereference	25-Mar-2023	5.5	A vulnerability, which was classified as problematic, was found in JiangMin Antivirus 16.2.2022.418. This affects the function 0x222010 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-224013 was assigned to this vulnerability. **CVE ID : CVE-2023-1631**	N/A	A-JIA-JIAN-050423/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: joommasters					
Product: jms_blog					
Affected Version(s): 2.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	PrestaShop jmsblog 2.5.5 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2023-27034**	https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html	A-JOO-JMS_-050423/813
Affected Version(s): 2.5.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	PrestaShop jmsblog 2.5.5 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2023-27034**	https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html	A-JOO-JMS_-050423/814
Vendor: joomunited					
Product: wp_meta_seo					
Affected Version(s): * Up to (excluding) 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	8.8	The WP Meta SEO WordPress plugin before 4.5.3 does not properly sanitize and escape inputs into SQL queries, leading to a blind SQL Injection vulnerability that can be exploited by subscriber+ users. **CVE ID : CVE-2023-0875**	N/A	A-JOO-WP_M-050423/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	20-Mar-2023	6.1	The WP Meta SEO WordPress plugin before 4.5.3 does not authorize several ajax actions, allowing low-privilege users to make updates to certain data and leading to an arbitrary redirect vulnerability. **CVE ID : CVE-2023-0876**	N/A	A-JOO-WP_M-050423/816
Vendor: json-smart_project					
Product: json-smart					
Affected Version(s): 2.4.9					
Uncontrolled Recursion	22-Mar-2023	7.5	[Json-smart](https://netplex.github.io/json-smart/) is a performance focused, JSON processor lib. When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively. It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software. **CVE ID : CVE-2023-1370**	N/A	A-JSO-JSON-050423/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: judging_management_system_project					
Product: judging_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability was found in SourceCodester Judging Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file summary_results.php. The manipulation of the argument main_event_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223549 was assigned to this vulnerability. **CVE ID : CVE-2023-1556**	N/A	A-JUD-JUDG-050423/818
Vendor: kaml_project					
Product: kaml					
Affected Version(s): * Up to (excluding) 0.53.0					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	20-Mar-2023	7.5	kaml provides YAML support for kotlinx.serialization. Prior to version 0.53.0, applications that use kaml to parse untrusted input containing anchors and aliases may consume excessive	https://github.com/charleskorn/kaml/security/advisories/GHSA-c24f-2j3g-rg48, https://github.com/c	A-KAM-KAML-050423/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Expansion')			memory and crash. Version 0.53.0 and later default to refusing to parse YAML documents containing anchors and aliases. There are no known workarounds. **CVE ID : CVE-2023-28118**	harleskorn/kaml/commit/5f82a2d7e00bfc307afca05d1dc4d7c50593531a	
Vendor: klaviyo					
Product: klaviyo					
Affected Version(s): * Up to (including) 3.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Klaviyo, Inc. Klaviyo plugin <= 3.0.7 versions. **CVE ID : CVE-2023-25456**	N/A	A-KLA-KLAV-050423/820
Vendor: knplabs					
Product: snappy					
Affected Version(s): * Up to (excluding) 1.4.2					
Deserialization of Untrusted Data	17-Mar-2023	9.8	Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any	https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc, https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c24442796	A-KNP-SNAP-050423/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the `generateFromHtml()` function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2. **CVE ID : CVE-2023-28115**	3fa2d92980b5d3, https://github.com/KnpLabs/snappy/commit/1ee6360cbdbea5d09705909a150df7963a88efd6	
Vendor: ladybirdweb					
Product: faveo_helpdesk					
Affected Version(s): From (including) 1.0 Up to (including) 1.11.1					
Improper Neutralization of Special Elements used in an SQL	24-Mar-2023	8.8	Faveo Helpdesk 1.0-1.11.1 is vulnerable to SQL Injection. When the user logs in through the login box, he has no judgment on the validity of the	N/A	A-LAD-FAVE-050423/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			user's input data. The parameters passed from the front end to the back end are controllable, which will lead to SQL injection. **CVE ID : CVE-2023-25350**		
Product: faveo_servicedesk					
Affected Version(s): 5.0.1					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	6.5	Faveo 5.0.1 allows remote attackers to obtain sensitive information via a modified user ID in an Insecure Direct Object Reference (IDOR) attack. **CVE ID : CVE-2023-24625**	N/A	A-LAD-FAVE-050423/823
Vendor: leadgenerated					
Product: lead_generated					
Affected Version(s): * Up to (excluding) 1.25					
Deserialization of Untrusted Data	22-Mar-2023	9.8	The Lead Generated WordPress Plugin, version <= 1.23, was affected by an unauthenticated insecure deserialization issue. The tve_labels parameter of the tve_api_form_submit action is passed to the PHP unserialize() function without being sanitized or verified, and as a result could lead to PHP object injection, which when	N/A	A-LEA-LEAD-050423/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			combined with certain class implementations / gadget chains could be leveraged to perform a variety of malicious actions granted a POP chain is also present. **CVE ID : CVE-2023-28667**		
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): * Up to (excluding) 2.2.1					
Path Traversal: '..filename'	24-Mar-2023	9.8	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.2.1. **CVE ID : CVE-2023-1177**	https://huntr.dev/bounties/1fe8f21a-c438-4cba-9add-e8a5dab94e28, https://github.com/mlflow/mlflow/commit/7162a50c654792c21f3e4a160eb1a0e6a34f6e6e	A-LFP-MLFL-050423/825
Affected Version(s): * Up to (excluding) 2.2.2					
Absolute Path Traversal	24-Mar-2023	3.3	Absolute Path Traversal in GitHub repository mlflow/mlflow prior to 2.2.2. **CVE ID : CVE-2023-1176**	https://huntr.dev/bounties/ae92f814-6a08-435c-8445-eec0ef4f1085, https://github.com/mlflow/mlflow/commit/	A-LFP-MLFL-050423/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				63ef72aa4334a6473ce7f889573c92fcae0b3c0d	
Vendor: liblouis					
Product: liblouis					
Affected Version(s): 3.24.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the lou_logFile function at logginc.c endpoint. **CVE ID : CVE-2023-26767**	https://github.com/liblouis/liblouis/issues/1292, https://github.com/liblouis/liblouis/pull/1297	A-LIB-LIBL-050423/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the compileTranslationTable.c and lou_setDataPath functions. **CVE ID : CVE-2023-26768**	https://github.com/liblouis/liblouis/pull/1302	A-LIB-LIBL-050423/828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis Lou_Trace v.3.24.0 allows a remote attacker to cause a denial of service via the resolveSubtable function at	https://github.com/liblouis/liblouis/pull/1300	A-LIB-LIBL-050423/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compileTranslationTabel.c. **CVE ID : CVE-2023-26769**		
Vendor: lightcms_project					
Product: lightcms					
Affected Version(s): 1.3.7					
N/A	22-Mar-2023	9.8	LightCMS v1.3.7 was discovered to contain a remote code execution (RCE) vulnerability via the image:make function. **CVE ID : CVE-2023-27060**	https://github.com/eddy8/LightCMS/issues/21	A-LIG-LIGH-050423/830
Vendor: loan_management_system_project					
Product: loan_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	5.4	SourceCodester Loan Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Type parameter under the Edit Loan Types module. **CVE ID : CVE-2023-27242**	N/A	A-LOA-LOAN-050423/831
Vendor: mage-people					
Product: event_manager_and_tickets_selling_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.8.7					
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin	N/A	A-MAG-EVEN-050423/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			for WooCommerce <= 3.8.6. versions. **CVE ID : CVE-2023-28422**		
Vendor: mainwp					
Product: code_snippets_extension					
Affected Version(s): * Up to (excluding) 4.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in MainWP MainWP Code Snippets Extension plugin <= 4.0.2 versions. **CVE ID : CVE-2023-23650**	N/A	A-MAI-CODE-050423/833
Vendor: Malwarebytes					
Product: adwcleaner					
Affected Version(s): * Up to (including) 8.4.0					
Improper Link Resolution Before File Access ('Link Following')	29-Mar-2023	7.8	Malwarebytes AdwCleaner 8.4.0 runs as Administrator and performs an insecure file delete operation on C:\AdwCleaner\Logs\AdwCleaner_Debug.log in which the target location is user-controllable, allowing a non-admin user to escalate privileges to SYSTEM via a symbolic link. **CVE ID : CVE-2023-28892**	https://www.malwarebytes.com/secure/cves/cve-2023-28892	A-MAL-ADWC-050423/834
Product: malwarebytes					
Affected Version(s): * Up to (excluding) 4.5.23					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	23-Mar-2023	7.8	In Malwarebytes before 4.5.23, a symbolic link may be used delete any arbitrary file on the system by exploiting the local quarantine system. It can also lead to privilege escalation in certain scenarios. **CVE ID : CVE-2023-26088**	https://www.malwarebytes.com/secure/cves/cve-2023-26088	A-MAL-MALW-050423/835
Vendor: mattermost					
Product: mattermost					
Affected Version(s): * Up to (excluding) 7.5.0					
Exposure of Resource to Wrong Sphere	22-Mar-2023	4.3	Mattermost fails to check the "Show Full Name" setting when rendering the result for the /plugins/focalboard/api/v2/users API call, allowing an attacker to learn the full name of a board owner. **CVE ID : CVE-2023-1562**	https://mattermost.com/security-updates/	A-MAT-MATT-050423/836
Vendor: maxpcsecure					
Product: anti_virus_plus					
Affected Version(s): 19.0.2.1					
Improper Access Control	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1 and classified as critical. Affected by this issue is the function 0x220020 in the library SDActMon.sys of the component	N/A	A-MAX-ANTI-050423/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IoControlCode Handler. The manipulation leads to improper access controls. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223376. **CVE ID : CVE-2023-1490**		
Improper Access Control	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been classified as critical. This affects the function 0x220020 in the library MaxCryptMon.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-223377 was assigned to this vulnerability. **CVE ID : CVE-2023-1491**	N/A	A-MAX-ANTI-050423/838
Improper Resource	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been	N/A	A-MAX-ANTI-050423/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			declared as problematic. This vulnerability affects the function 0x220019 in the library MaxProc64.sys of the component IoControlCode Handler. The manipulation of the argument SystemBuffer leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-223378 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1492**		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been rated as problematic. This issue affects the function 0x220019 in the library MaxProctetor64.sys of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated	N/A	A-MAX-ANTI-050423/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-223379. **CVE ID : CVE-2023-1493**		
Vendor: Mcafee					
Product: total_protection					
Affected Version(s): * Up to (excluding) 16.0.50					
N/A	21-Mar-2023	6.7	McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific Component Object Model (COM) in the Windows Registry. This can result in the loading of a malicious payload. **CVE ID : CVE-2023-25134**	https://www.mcafee.com/support/?articleId=TS103398&page=shell&shell=article-view, https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html	A-MCA-TOTA-050423/841
Vendor: medical_certificate_generator_app_project					
Product: medical_certificate_generator_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the	N/A	A-MED-MEDI-050423/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223558 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1566**		
Vendor: medicine_tracker_system_project					
Product: medicine_tracker_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Medicine Tracker System 1.0. This issue affects some unknown processing of the file medicines/view_details.php of the component GET Parameter Handler. The manipulation of the argument GET leads to sql injection. 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-223283. **CVE ID : CVE-2023-1439**	N/A	A-MED-MEDI-050423/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file Users.php?f=save_user. The manipulation of the argument firstname/middlename/lastname/username/password leads to improper authentication. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223311. **CVE ID : CVE-2023-1464**	N/A	A-MED-MEDI-050423/844
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Medicine Tracker System 1.0. Affected by this issue is some unknown functionality of the file app/?page=medicines/manage_medicine. The manipulation of the argument name/description with the input <script>alert('2')</script> leads to cross site scripting. The attack may be launched	N/A	A-MED-MEDI-050423/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The identifier of this vulnerability is VDB-223292. **CVE ID : CVE-2023-1447**		
Vendor: megamain					
Product: mega_main_menu					
Affected Version(s): * Up to (including) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	4.8	The Mega Main Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, 2.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1575**	N/A	A-MEG-MEGA-050423/846
Vendor: menu_shortcode_project					
Product: menu_shortcode					
Affected Version(s): * Up to (including) 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The menu shortcode WordPress plugin through 1.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0395**	N/A	A-MEN-MENU-050423/847
Vendor: metagauss					
Product: profilegrid					
Affected Version(s): * Up to (excluding) 5.3.1					
Incorrect Authorization	20-Mar-2023	8.8	The ProfileGrid WordPress plugin before 5.3.1 provides an AJAX endpoint for resetting a user password but does not implement proper authorization. This allows a user with low privileges, such as subscriber, to change the password of any account, including Administrator ones. **CVE ID : CVE-2023-0940**	N/A	A-MET-PROF-050423/848
Vendor: mgt-commerce					
Product: cloudpanel					
Affected Version(s): * Up to (excluding) 2.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	21-Mar-2023	8.1	MGT-COMMERCE CloudPanel ships with a static SSL certificate to encrypt communications to the administrative interface, shared across every installation of CloudPanel. This behavior was observed in version 2.2.0. There has been no indication from the vendor this has been addressed in version 2.2.1. **CVE ID : CVE-2023-0391**	N/A	A-MGT-CLOU-050423/849
Vendor: miniflux_project					
Product: miniflux					
Affected Version(s): * Up to (excluding) 2.0.43					
N/A	17-Mar-2023	7.5	Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheus metrics from a publicly reachable Miniflux instance where the `METRICS_COLLECTOR` configuration option is enabled and `METRICS_ALLOWED_NETWORKS` is set to `127.0.0.1/8` (the default). A patch is available in Miniflux 2.0.43. As a workaround, set `METRICS_COLLECTO	https://github.com/miniflux/v2/security/advisories/GHSA-3qjf-qh38-x73v, https://github.com/miniflux/v2/pull/1745	A-MIN-MINI-050423/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R` to `false` (default) or run Miniflux behind a trusted reverse-proxy. **CVE ID : CVE-2023-27591**		
Affected Version(s): From (including) 2.0.25 Up to (excluding) 2.0.43					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Miniflux is a feed reader. Since v2.0.25, Miniflux will automatically proxy images served over HTTP to prevent mixed content errors. When an outbound request made by the Go HTTP client fails, the `html.ServerError` is returned unescaped without the expected Content Security Policy header added to valid responses. By creating an RSS feed item with the inline description containing an `<img>` tag with a `srcset` attribute pointing to an invalid URL like `http:a<script>alert(1)</script>`, we can coerce the proxy handler into an error condition where the invalid URL is returned unescaped and in full. This results in JavaScript execution on the Miniflux instance as soon as the user is convinced (e.g. by a	https://github.com/miniflux/v2/pull/1746, https://github.com/miniflux/v2/security/advisories/GHSA-mqqg-xjhj-wfgw	A-MIN-MINI-050423/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in the alt text) to open the broken image. An attacker can execute arbitrary JavaScript in the context of a victim Miniflux user when they open a broken image in a crafted RSS feed. This can be used to perform actions on the Miniflux instance as that user and gain administrative access to the Miniflux instance if it is reachable and the victim is an administrator. A patch is available in version 2.0.43. As a workaround sisable image proxy; default value is `http-only`. **CVE ID : CVE-2023-27592**		
Vendor: minio					
Product: minio					
Affected Version(s): * Up to (excluding) 2023-03-20t20-16-18z					
N/A	22-Mar-2023	8.8	Minio is a Multi-Cloud Object Storage framework. All users on Windows prior to version RELEASE.2023-03-20T20-16-18Z are impacted. MinIO fails to filter the `\` character, which allows for arbitrary object placement across buckets. As a	https://github.com/minio/minio/commit/8d6558b23649f613414c8527b58973fbdfa4d1b8, https://github.com/minio/minio/security/a	A-MIN-MINI-050423/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result, a user with low privileges, such as an access key, service account, or STS credential, which only has permission to `PutObject` in a specific bucket, can create an admin user. This issue is patched in RELEASE.2023-03-20T20-16-18Z. There are no known workarounds. **CVE ID : CVE-2023-28433**	dvisories/GHSA-w23q-4hw3-2pp6, https://github.com/minio/minio/commit/b3c54ec81e0a06392abfb3a1ffcdc80c6fbf6ebc	
N/A	22-Mar-2023	8.8	Minio is a Multi-Cloud Object Storage framework. Prior to RELEASE.2023-03-20T20-16-18Z, an attacker can use crafted requests to bypass metadata bucket name checking and put an object into any bucket while processing `PostPolicyBucket`. To carry out this attack, the attacker requires credentials with `arn:aws:s3:::*` permission, as well as enabled Console API access. This issue has been patched in RELEASE.2023-03-20T20-16-18Z. As a workaround, enable browser API access and turn off	https://github.com/minio/minio/security/advisories/GHSA-2pxw-r47w-4p8c, https://github.com/minio/minio/commit/67f4ba154a27a1b06e48bfabda38355a010dfca5	A-MIN-MINI-050423/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`MINIO_BROWSER=off`. **CVE ID : CVE-2023-28434**		
Affected Version(s): From (including) 2019-12-17t23-16-33z Up to (excluding) 2023-03-20t20-16-18z					
N/A	22-Mar-2023	7.5	Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z. **CVE ID : CVE-2023-28432**	https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q	A-MIN-MINI-050423/854
Vendor: miniorange					
Product: oauth_single_sign_on					
Affected Version(s): * Up to (excluding) 6.24.2					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The OAuth Single Sign On WordPress plugin before 6.24.2 does not have CSRF checks when discarding	N/A	A-MIN-OAUT-050423/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Identify providers (IdP), which could allow attackers to make logged in admins delete all IdP via a CSRF attack **CVE ID : CVE-2023-1093**		
Vendor: mirotalk					
Product: mirotalk_p2p					
Affected Version(s): * Up to (excluding) 2023-02-18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in MiroTalk P2P before commit f535b35 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter under the settings module. **CVE ID : CVE-2023-27054**	https://github.com/miroslavpejic85/mirotalk/issues/139, https://github.com/miroslavpejic85/mirotalk/commit/f535b3515d2d480dc3135b37982f5df93e43c592	A-MIR-MIRO-050423/856
Vendor: Misp-project					
Product: malware_information_sharing_platform					
Affected Version(s): * Up to (excluding) 2.4.169					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	js/event-graph.js in MISP before 2.4.169 allows XSS via event-graph node tooltips. **CVE ID : CVE-2023-28606**	https://github.com/MISP/MISP/commit/30255b8d683df4ec54f856282b3bde9106d5ae1a	A-MIS-MALW-050423/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	js/event-graph.js in MISP before 2.4.169 allows XSS via the event-graph relationship tooltip. **CVE ID : CVE-2023-28607**	https://github.com/MISP/MISP/commit/78f423451a4c795991e739ee970bc5215c061591	A-MIS-MALW-050423/858
Affected Version(s): 2.4.169					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	In MISP 2.4.169, app/Lib/Tools/CustomPaginationTool.php allows XSS in the community index. **CVE ID : CVE-2023-28884**	https://github.com/MISP/MISP/commit/b94c7978e5e6b1db369abeedbbf00bca975b08b7	A-MIS-MALW-050423/859
Vendor: monitoring_of_students_cyber_accounts_system_project					
Product: monitoring_of_students_cyber_accounts_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Parameter Handler. The manipulation of the argument un leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be	N/A	A-MON-MONI-050423/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The associated identifier of this vulnerability is VDB-223363. **CVE ID : CVE-2023-1480**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this issue is some unknown functionality of the file modules/balance/index.php?view=balancelist of the component POST Parameter Handler. The manipulation of the argument id with the input "><script>alert(111)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223364. **CVE ID : CVE-2023-1481**	N/A	A-MON-MONI-050423/861
Vendor: monospace					
Product: directus					
Affected Version(s): * Up to (excluding) 9.23.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	24-Mar-2023	5.5	Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.23.3, the `directus_refresh_token` is not redacted properly from the log outputs and can be used to impersonate users without their permission. This issue is patched in version 9.23.3. **CVE ID : CVE-2023-28443**	https://github.com/directus/directus/security/advisories/GHSA-8vg2-wf3q-mwv7, https://github.com/directus/directus/commit/349536303983ccba68ecb3e4fb35315424011afc	A-MON-DIRE-050423/862
Vendor: Moodle					
Product: moodle					
Affected Version(s): 4.1.1					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/863
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers).	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2023-28329**		
Cross-Site Request Forgery (CSRF)	23-Mar-2023	8.8	The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk. **CVE ID : CVE-2023-28335**	https://moodle.org/mod/forum/discuss.php?d=445067	A-MOO-MOOD-050423/865
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/866
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/867
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. **CVE ID : CVE-2023-28332**	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/868
Exposure of Resource	23-Mar-2023	4.3	The course participation report required additional	https://moodle.org/mod/forum/	A-MOO-MOOD-050423/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	discuss.php?d=445069	
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. **CVE ID : CVE-2023-28334**	https://moodle.org/mod/forum/discuss.php?d=445066	A-MOO-MOOD-050423/870
Affected Version(s): 3.11.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/871
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/872
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/874
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. **CVE ID : CVE-2023-28332**	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/875
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/876
Affected Version(s): 3.9.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploita	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ble anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/878
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/879
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/880
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-28332**		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/882
Affected Version(s): 4.0.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/883
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/884
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			teachers, managers and admins by default. **CVE ID : CVE-2023-28330**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/886
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. **CVE ID : CVE-2023-28332**	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/887
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/888
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. **CVE ID : CVE-2023-28334**	https://moodle.org/mod/forum/discuss.php?d=445066	A-MOO-MOOD-050423/889
Affected Version(s): 4.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/890
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/891
Cross-Site Request Forgery (CSRF)	23-Mar-2023	8.8	The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk. **CVE ID : CVE-2023-28335**	https://moodle.org/mod/forum/discuss.php?d=445067	A-MOO-MOOD-050423/892
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/894
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. **CVE ID : CVE-2023-28332**	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/895
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/896
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. **CVE ID : CVE-2023-28334**	https://moodle.org/mod/forum/discuss.php?d=445066	A-MOO-MOOD-050423/897
Affected Version(s): From (excluding) 3.11.0 Up to (excluding) 3.11.13					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/899
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/900
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/901
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			server), it presented an XSS risk. **CVE ID : CVE-2023-28332**		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/903
Affected Version(s): From (excluding) 3.9.0 Up to (excluding) 3.9.20					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/904
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/905
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/907
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. **CVE ID : CVE-2023-28332**	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/908
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/909
Affected Version(s): From (excluding) 4.0.0 Up to (excluding) 4.0.7					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploita	https://moodle.org/mod/forum/discuss.php?d=445065	A-MOO-MOOD-050423/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ble anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). **CVE ID : CVE-2023-28329**	https://moodle.org/mod/forum/discuss.php?d=445061	A-MOO-MOOD-050423/911
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. **CVE ID : CVE-2023-28330**	https://moodle.org/mod/forum/discuss.php?d=445062	A-MOO-MOOD-050423/912
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. **CVE ID : CVE-2023-28331**	https://moodle.org/mod/forum/discuss.php?d=445063	A-MOO-MOOD-050423/913
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.	https://moodle.org/mod/forum/discuss.php?d=445064	A-MOO-MOOD-050423/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-28332**		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. **CVE ID : CVE-2023-1402**	https://moodle.org/mod/forum/discuss.php?d=445069	A-MOO-MOOD-050423/915
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. **CVE ID : CVE-2023-28334**	https://moodle.org/mod/forum/discuss.php?d=445066	A-MOO-MOOD-050423/916
Vendor: mp4v2_project					
Product: mp4v2					
Affected Version(s): 2.1.2					
Improper Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability was found in MP4v2 2.1.2 and classified as problematic. This issue affects the function DumpTrack of the file mp4trackdump.cpp. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223295.	N/A	A-MP4-MP4V-050423/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1450		
Improper Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability was found in MP4v2 2.1.2. It has been classified as problematic. Affected is the function mp4v2::impl::MP4Track::GetSampleFileOffset of the file mp4track.cpp. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223296. **CVE ID : CVE-2023-1451**	N/A	A-MP4-MP4V-050423/918
Vendor: Netgate					
Product: Pfsense					
Affected Version(s): 2.7.0					
XML Injection (aka Blind XPath Injection)	17-Mar-2023	8.8	A command injection vulnerability in the function restore_rrddata() of Netgate pfSense v2.7.0 allows authenticated attackers to execute arbitrary commands via manipulating the contents of an XML file supplied to the component config.xml. **CVE ID : CVE-2023-27253**	https://redmine.pfsense.org/issues/13935, https://github.com/pfsense/pfsense/commit/ca80d18493f8f91b21933ebd6b714215ae1e5e94	A-NET-PFSE-050423/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pfsense_plus					
Affected Version(s): 22.05.1					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	9.8	Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v22.05.1 and pfSense CE software v2.6.0 allows attackers to bypass brute force protection mechanisms via crafted web requests. **CVE ID : CVE-2023-27100**	https://redmine.pfsense.org/issues/13574, https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc	A-NET-PFSE-050423/920
Vendor: Nextcloud					
Product: nextcloud_server					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x, https://github.com/nextcloud/server/pull/36489	A-NEX-NEXT-050423/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25820**		
Affected Version(s): From (including) 22.2.0 Up to (excluding) 22.2.10.10					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x, https://github.com/nextcloud/server/pull/36489	A-NEX-NEXT-050423/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25820**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.5					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x, https://github.com/nextcloud/server/pull/36489	A-NEX-NEXT-050423/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25820**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.10					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x, https://github.com/nextcloud/server/pull/36489	A-NEX-NEXT-050423/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-25820**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.9					
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	8.1	Nextcloud server is an open source, personal cloud implementation. In versions from 24.0.0 and before 24.0.9 a user could escalate their permissions to delete files they were not supposed to deletable but only viewed or downloaded. This issue has been addressed andit is recommended that the Nextcloud Server is upgraded to 24.0.9. There are no known workarounds for this vulnerability.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8v5c-f752-fgpv, https://github.com/nextcloud/server/pull/33941	A-NEX-NEXT-050423/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25817		
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.4					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10, when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-36g6-wjx2-333x, https://github.com/nextcloud/server/pull/36489	A-NEX-NEXT-050423/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25820		
Vendor: Nextendweb					
Product: smart_slider_3					
Affected Version(s): * Up to (excluding) 3.5.1.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Smart Slider 3 WordPress plugin before 3.5.1.14 does not properly validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0660**	N/A	A-NEX-SMAR-050423/927
Vendor: nooz_project					
Product: nooz					
Affected Version(s): * Up to (including) 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Mighty Digital Nooz plugin <= 1.6.0 versions. **CVE ID : CVE-2023-25794**	N/A	A-NOO-NOOZ-050423/928
Vendor: notrinos					
Product: notrinoserp					
Affected Version(s): 0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	RESERVED NotrinosERP v0.7 was discovered to contain a SQL injection vulnerability via the OrderNumber parameter at /NotrinosERP/sales/customer_delivery.php. **CVE ID : CVE-2023-24788**	N/A	A-NOT-NOTR-050423/929
Vendor: novel-plus_project					
Product: novel-plus					
Affected Version(s): 3.6.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in novel-plus 3.6.2. Affected is the function MenuService of the file sys/menu/list. The manipulation of the argument sort 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-223662 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1594**	N/A	A-NOV-NOVE-050423/930
Improper Neutralization of Special Elements used in an SQL	23-Mar-2023	9.8	A vulnerability was found in novel-plus 3.6.2 and classified as critical. Affected by this issue is some unknown functionality of the file	N/A	A-NOV-NOVE-050423/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			DictController.java. The manipulation of the argument orderby 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-223736. **CVE ID : CVE-2023-1606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	A vulnerability was found in novel-plus 3.6.2. It has been classified as critical. This affects an unknown part of the file /common/sysFile/list. The manipulation of the argument sort 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-223737 was assigned to this vulnerability. **CVE ID : CVE-2023-1607**	N/A	A-NOV-NOVE-050423/932
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	7.2	A vulnerability has been found in novel-plus 3.6.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file	N/A	A-NOV-NOVE-050423/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			common/log/list. The manipulation of the argument sort 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-223663. **CVE ID : CVE-2023-1595**		
Vendor: nsthemes					
Product: advanced_social_pixel					
Affected Version(s): * Up to (including) 2.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NsThemes Advanced Social Pixel plugin <= 2.1.1 versions. **CVE ID : CVE-2023-24381**	N/A	A-NST-ADVA-050423/934
Vendor: ofcms_project					
Product: ofcms					
Affected Version(s): 1.1.4					
Improper Privilege Management	16-Mar-2023	8.8	An issue found in Ofcms v.1.1.4 allows a remote attacker to to escalate privileges via the respwd method in SysUserController. **CVE ID : CVE-2023-24760**	https://gitee.com/oufu/ofcms/issues/I6L75S	A-OFC-OFCM-050423/935
Vendor: omicronenergy					
Product: stationguard					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.20					
N/A	23-Mar-2023	9.8	The update process in OMICRON StationGuard and OMICRON StationScout before 2.21 can be exploited by providing a modified firmware update image. This allows a remote attacker to gain root access to the system. **CVE ID : CVE-2023-28610**	https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-5.txt, https://www.omicronenergy.com/en/support/product-security/	A-OMI-STAT-050423/936
Affected Version(s): From (including) 1.10 Up to (including) 2.20					
Incorrect Authorization	23-Mar-2023	9.8	Incorrect authorization in OMICRON StationGuard 1.10 through 2.20 and StationScout 1.30 through 2.20 allows an attacker to bypass intended access restrictions. **CVE ID : CVE-2023-28611**	https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-6.txt, https://www.omicronenergy.com/en/support/product-security/	A-OMI-STAT-050423/937
Product: stationscout					
Affected Version(s): * Up to (including) 2.20					
N/A	23-Mar-2023	9.8	The update process in OMICRON StationGuard and OMICRON StationScout before 2.21 can be exploited	https://www.omicronenergy.com/fileadmin/user_upload/website/	A-OMI-STAT-050423/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by providing a modified firmware update image. This allows a remote attacker to gain root access to the system. **CVE ID : CVE-2023-28610**	files/product-security/osa-5.txt, https://www.omicronenergy.com/en/support/product-security/	
Affected Version(s): From (including) 1.30 Up to (including) 2.20					
Incorrect Authorization	23-Mar-2023	9.8	Incorrect authorization in OMICRON StationGuard 1.10 through 2.20 and StationScout 1.30 through 2.20 allows an attacker to bypass intended access restrictions. **CVE ID : CVE-2023-28611**	https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-6.txt, https://www.omicronenergy.com/en/support/product-security/	A-OMI-STAT-050423/939
Vendor: onekeyadmin					
Product: onekeyadmin					
Affected Version(s): 1.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Member List module. **CVE ID : CVE-2023-26951**	N/A	A-ONE-ONEK-050423/940
Vendor: online_book_store_project_project					
Product: online_book_store_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	Online Book Store Project v1.0 is vulnerable to SQL Injection via /bookstore/bookPerPub.php. **CVE ID : CVE-2023-27250**	https://github.com/iknownt/bug_report/blob/main/vendors/itsourcecode.com/Online-Book-Store-Project/sql_injection.md	A-ONL-ONLI-050423/941
Vendor: online_exam_software_					
Product: _eexamhall_project					
Affected Version(s): online_exam_software_\\ Up to (including) 4.0					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Aarvanshinfotech Online Exam Software: eExamhall plugin <= 4.0 versions. **CVE ID : CVE-2023-22681**	N/A	A-ONL-_EEX-050423/942
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 2.0					
Improper Access Control	16-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Food Ordering System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /fos/admin/ajax.php?action=save_settings	N/A	A-ONL-ONLI-050423/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be launched remotely. VDB-223214 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1432**		
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file admin/ajax.php?action=login2 of the component Login Page. The manipulation of the argument email with the input abc%40qq.com' AND (SELECT 9110 FROM (SELECT(SLEEP(5)))XSlc) AND 'jFNl'='jFNl leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-ONL-ONLI-050423/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-223300. **CVE ID : CVE-2023-1455**		
Improper Authentication	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file admin/ajax.php?action=save_user of the component Password Change Handler. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The identifier VDB-223305 was assigned to this vulnerability. **CVE ID : CVE-2023-1460**	N/A	A-ONL-ONLI-050423/945
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability has been found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This vulnerability affects the function exec of the file admin/operations/ap	N/A	A-ONL-ONLI-050423/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prove_delete.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223654 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1589**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects the function exec of the file admin/operations/currency.php. The manipulation of the argument id leads to sql injection. 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-223655. **CVE ID : CVE-2023-1590**	N/A	A-ONL-ONLI-050423/947
Vendor: ooohboi_steroids_for_elementor_project					
Product: ooohboi_steroids_for_elementor					
Affected Version(s): * Up to (excluding) 2.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The OoohBoi Steroids for Elementor WordPress plugin before 2.1.5 has CSRF and broken access control vulnerabilities which leads user with role as low as subscriber to delete attachment. **CVE ID : CVE-2023-0336**	N/A	A-OOO-OOOH-050423/948
Vendor: oopspam					
Product: oopspam_anti-spam					
Affected Version(s): * Up to (excluding) 1.1.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting vulnerability in OOPSpam OOPSpam Anti-Spam plugin <= 1.1.35 versions. **CVE ID : CVE-2023-22716**	N/A	A-OOP-OOPS-050423/949
Vendor: Openbsd					
Product: openssh					
Affected Version(s): * Up to (excluding) 9.3					
N/A	17-Mar-2023	9.8	ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. **CVE ID : CVE-2023-28531**	N/A	A-OPE-OPEN-050423/950
Vendor: openfind					
Product: mail2000					
Affected Version(s): 8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	Openfind Mail2000 file uploading function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject JavaScript, conducting an XSS attack. **CVE ID : CVE-2023-22902**	https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html	A-OPE-MAIL-050423/951
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	Openfind Mail2000 file uploading function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject JavaScript, conducting an XSS attack. **CVE ID : CVE-2023-22902**	https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html	A-OPE-MAIL-050423/952
Vendor: opengoofy					
Product: hippo4j					
Affected Version(s): * Up to (excluding) 1.4.3					
Incorrect Permission Assignment for Critical Resource	16-Mar-2023	6.5	Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker toescalate privileges via the AddUser method of the UserController function in Tenant Management module.	N/A	A-OPE-HIPP-050423/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27095		
Affected Version(s): 1.4.3					
N/A	23-Mar-2023	8.8	An issue found in OpenGoofy Hippo4j v.1.4.3 allows attackers to escalate privileges via the ThreadPoolController of the tenant Management module. **CVE ID : CVE-2023-27094**	https://github.com/opengoofy/hippo4j/issues/1059	A-OPE-HIPP-050423/954
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	6.5	Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker to obtain sensitive information via the ConfigVerifyController function of the Tenant Management module. **CVE ID : CVE-2023-27096**	https://github.com/opengoofy/hippo4j/issues/1060	A-OPE-HIPP-050423/955
Vendor: Opennms					
Product: horizon					
Affected Version(s): * Up to (excluding) 31.0.6					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian	https://github.com/OpenNMS/opennms/pull/5835/files	A-OPE-HORI-050423/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. **CVE ID : CVE-2023-0870**		
Product: meridian					
Affected Version(s): 2023.1.0					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	https://github.com/OpenNMS/opennms/pull/5835/files	A-OPE-MERI-050423/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0870		
Affected Version(s): From (including) 2020.1.0 Up to (excluding) 2020.1.33					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. **CVE ID : CVE-2023-0870**	https://github.com/OpenNMS/opennms/pull/5835/files	A-OPE-MERI-050423/958
Affected Version(s): From (including) 2021.1.0 Up to (excluding) 2021.1.25					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential	https://github.com/OpenNMS/opennms/pull/5835/files	A-OPE-MERI-050423/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. **CVE ID : CVE-2023-0870**		
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.14					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly	https://github.com/OpenNMS/opennms/pull/5835/files	A-OPE-MERI-050423/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible from the Internet. **CVE ID : CVE-2023-0870**		
Vendor: Openssl					
Product: openssl					
Affected Version(s): From (including) 1.0.2 Up to (excluding) 1.0.2zh					
Improper Certificate Validation	22-Mar-2023	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. **CVE ID : CVE-2023-0464**	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1, https://www.openssl.org/news/secadv/20230322.txt	A-OPE-OPEN-050423/961
Affected Version(s): From (including) 1.1.1 Up to (excluding) 1.1.1u					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	22-Mar-2023	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. **CVE ID : CVE-2023-0464**	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1, https://www.openssl.org/news/secadv/20230322.txt	A-OPE-OPEN-050423/962
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.9					
Improper Certificate Validation	22-Mar-2023	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545,	A-OPE-OPEN-050423/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. **CVE ID : CVE-2023-0464**	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1, https://www.openssl.org/news/secadv/20230322.txt	
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.1					
Improper Certificate Validation	22-Mar-2023	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems.	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1,	A-OPE-OPEN-050423/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. **CVE ID : CVE-2023-0464**	https://www.openssl.org/news/secadv/20230322.txt	
Vendor: otcms					
Product: otcms					
Affected Version(s): 6.72					
Server-Side Request Forgery (SSRF)	25-Mar-2023	9.8	A vulnerability was found in OTCMS 6.72. It has been classified as critical. Affected is the function UseCurl of the file /admin/info_deal.php of the component URL Parameter Handler. The manipulation leads to server-side request forgery. 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-224016. **CVE ID : CVE-2023-1634**	N/A	A-OTC-OTCM-050423/965
Improper Neutralization of Input During	25-Mar-2023	6.1	A vulnerability was found in OTCMS 6.72. It has been declared as problematic. Affected by this vulnerability is	N/A	A-OTC-OTCM-050423/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the function AutoRun of the file apiRun.php. The manipulation of the argument mode leads to cross site scripting. The attack can be launched remotely. The identifier VDB-224017 was assigned to this vulnerability. **CVE ID : CVE-2023-1635**		
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 6.0.1 Up to (including) 6.0.34					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2023-1250**	https://otrs.com/release-notes/otrs-security-advisory-2023-02/	A-OTR-OTRS-050423/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	Improper Input Validation vulnerability in OTRS AG OTRS (Ticket Actions modules), OTRS AG ((OTRS)) Community Edition (Ticket Actions modules) allows Cross-Site Scripting (XSS).This issue affects OTRS: from 7.0.X before 7.0.42; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2023-1248**	https://otrs.com/release-notes/otrs-security-advisory-2023-01/	A-OTR-OTRS-050423/968
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.42					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	https://otrs.com/release-notes/otrs-security-advisory-2023-02/	A-OTR-OTRS-050423/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1250		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	Improper Input Validation vulnerability in OTRS AG OTRS (Ticket Actions modules), OTRS AG ((OTRS)) Community Edition (Ticket Actions modules) allows Cross-Site Scripting (XSS).This issue affects OTRS: from 7.0.X before 7.0.42; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2023-1248**	https://otrs.com/release-notes/otrs-security-advisory-2023-01/	A-OTR-OTRS-050423/970
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.31					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition:	https://otrs.com/release-notes/otrs-security-advisory-2023-02/	A-OTR-OTRS-050423/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 6.0.1 through 6.0.34. **CVE ID : CVE-2023-1250**		
Vendor: pacsrapor					
Product: pacsrapor					
Affected Version(s): * Up to (excluding) 1.22					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pacsrapor allows SQL Injection, Command Line Execution through SQL Injection.This issue affects Pacsrapor: before 1.22. **CVE ID : CVE-2023-1153**	N/A	A-PAC-PACS-050423/972
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pacsrapor allows Reflected XSS.This issue affects Pacsrapor: before 1.22. **CVE ID : CVE-2023-1154**	N/A	A-PAC-PACS-050423/973
Vendor: page_loading_effects_project					
Product: page_loading_effects					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralizat	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS)	N/A	A-PAG-PAGE-050423/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Esstat17 Page Loading Effects plugin <= 2.0.0 versions. **CVE ID : CVE-2023-23718**		
Vendor: parity					
Product: frontier					
Affected Version(s): * Up to (excluding) 2023-03-15					
Incorrect Calculation	22-Mar-2023	7.5	Frontier is an Ethereum compatibility layer for Substrate. Frontier's `modexp` precompile uses `num-bigint` crate under the hood. In the implementation prior to pull request 1017, the cases for modulus being even and modulus being odd are treated separately. Odd modulus uses the fast Montgomery multiplication, and even modulus uses the slow plain power algorithm. This gas cost discrepancy was not accounted for in the `modexp` precompile, leading to possible denial of service attacks. No fixes for `num-bigint` are currently available, and thus this issue is fixed in the short term by raising the gas costs for even modulus, and	https://github.com/paritytech/frontier/pull/1017, https://github.com/paritytech/frontier/commit/5af12e94d7dfc8a0208a290643a800f55de7b219, https://github.com/paritytech/frontier/security/advisories/GHSA-fcmm-54jp-7vf6	A-PAR-FRON-050423/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the long term fixing it in `num-bigint` or switching to another modexp implementation. The short-term fix for Frontier is deployed at pull request 1017. There are no known workarounds aside from applying the fix. **CVE ID : CVE-2023-28431**		
Vendor: park_ticketing_management_system_project					
Product: park_ticketing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	9.8	Phpgurukul Park Ticketing Management System 1.0 is vulnerable to SQL Injection via the User Name parameter. **CVE ID : CVE-2023-26959**	N/A	A-PAR-PARK-050423/976
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	Phpgurukul Park Ticketing Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Admin Name parameter. **CVE ID : CVE-2023-26958**	N/A	A-PAR-PARK-050423/977
Vendor: pdfio_project					
Product: pdfio					
Affected Version(s): * Up to (excluding) 1.1.1					
Allocation of	20-Mar-2023	3.3	PDFio is a C library for reading and writing	https://github.com/m	A-PDF-PDFI-050423/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resources Without Limits or Throttling			PDF files. In versions 1.1.0 and prior, a denial of service vulnerability exists in the pdfio parser. Crafted pdf files can cause the program to run at 100% utilization and never terminate. This is different from CVE-2023-24808. A patch for this issue is available in version 1.1.1. **CVE ID : CVE-2023-28428**	ichaelrsweet/pdfio/security/advisories/GHSA-68x8-9phf-j7jf, https://github.com/michaelrsweet/pdfio/commit/97d4955666779dc5b0665e15dd951a5c12426a31	
Vendor: Pfsense					
Product: pfsense					
Affected Version(s): 2.6.0					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	9.8	Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v22.05.1 and pfSense CE software v2.6.0 allows attackers to bypass brute force protection mechanisms via crafted web requests. **CVE ID : CVE-2023-27100**	https://redmine.pfsense.org/issues/13574, https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc	A-PFS-PFSE-050423/979
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.19					
Improper Neutralization of	22-Mar-2023	8.8	SQL Injection in GitHub repository	https://huntr.dev/bounties/7e4	A-PIM-PIMC-050423/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1578**	41a14-8e55-4ab4-932c-4dc56bb1bc2e, https://github.com/pimcore/pimcore/commit/367b74488808d71ec3f66f4ca9e8df5217c2c8d2	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, since a user with 'report' permission can already write arbitrary SQL queries and given the fact that this endpoint is using the GET method (no CSRF protection), an attacker can inject an arbitrary query by manipulating a user to click on a link. Users should upgrade to version 10.5.19 to receive a patch or, as a workaround, may apply the patch manually. **CVE ID : CVE-2023-28438**	https://github.com/pimcore/pimcore/security/advisories/GHSA-vf7q-g2pv-jxvx, https://github.com/pimcore/pimcore/pull/14526, https://github.com/pimcore/pimcore/commit/d1abadb181c88ebaa4bce1916f9077469d4ea2bc.patch	A-PIM-PIMC-050423/981
Improper Neutralization of	16-Mar-2023	7.8	Pimcore is an open source data and experience	https://github.com/pimcore/pim	A-PIM-PIMC-050423/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			management platform. Prior to version 10.5.19, quoting is not done properly in UUID DAO model. There is the theoretical possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting being done by the DAO class. Users should update to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually. **CVE ID : CVE-2023-28108**	core/security/advisories/GHSA-xc9p-r5qj-8xm9, https://github.com/pimcore/pimcore/commit/08e7ba56ae983c3c67ec563b6989b16ef8f35275.patch, https://github.com/pimcore/pimcore/pull/14633	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	Pimcore is an open source data and experience management platform. Versions prior to 10.5.19 have an unsecured tooltip field in DataObject class definition. This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie or redirect users to other malicious sites. Users should upgrade to version 10.5.19 or, as	https://github.com/pimcore/pimcore/pull/14574.patch, https://github.com/pimcore/pimcore/security/advisories/GHSA-rcg9-hrhx-6q69, https://github.com/pimcore/pimcore/pull/14574	A-PIM-PIMC-050423/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a workaround, apply the patch manually. **CVE ID : CVE-2023-28429**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1429**	https://huntr.dev/bounties/e0829fea-e458-47b8-84a3-a74476d9638f, https://github.com/pimcore/pimcore/commit/7588c336edb24050656111b89d69e69cc9feb5f5	A-PIM-PIMC-050423/984
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1515**	https://huntr.dev/bounties/ae0f2ec4-a245-4d0b-9d4d-bd8310dd6282, https://github.com/pimcore/pimcore/commit/44c6b37aa649a0e3105fa41f3d74a3e511acf964	A-PIM-PIMC-050423/985
Improper Neutralization of Input During	20-Mar-2023	4.8	Cross-site Scripting (XSS) - DOM in GitHub repository	https://huntr.dev/bounties/82adf0dd-8ebd-4d15-	A-PIM-PIMC-050423/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1517**	9f91-6060c8fa5a0d, https://github.com/pimcore/pimcore/commit/3a22700dacd8a439cffcb208838a4199e732cff7	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, an attacker can use cross-site scripting to send a malicious script to an unsuspecting user. Users may upgrade to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually. **CVE ID : CVE-2023-28106**	https://github.com/pimcore/pimcore/commit/c59d0bf1d03a5037b586fe06230694fa3818dbf2, https://github.com/pimcore/pimcore/pull/14669.patch, https://github.com/pimcore/pimcore/security/advisories/GHSA-x5j3-mq9g-8jc8	A-PIM-PIMC-050423/987
Vendor: pixedelic					
Product: camera_slideshow					
Affected Version(s): * Up to (including) 1.4.0.1					
Improper Neutralization of Input During	20-Mar-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in Manuel Masia | Pixedelic.Com Camera	N/A	A-PIX-CAME-050423/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			slideshow plugin <= 1.4.0.1 versions. **CVE ID : CVE-2023-22682**		
Vendor: play-with-docker					
Product: play_with_docker					
Affected Version(s): 0.0.1					
Authorization Bypass Through User-Controlled Key	16-Mar-2023	6.5	Play With Docker is a browser-based Docker playground. Versions 0.0.2 and prior are vulnerable to domain hijacking. Because CORS configuration was not correct, an attacker could use `play-with-docker.com` as an example and set the origin header in an http request as `evil-play-with-docker.com`. The domain would echo in response header, which successfully bypassed the CORS policy and retrieved basic user information. This issue has been fixed in commit ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a. There are no known workarounds. **CVE ID : CVE-2023-28109**	https://github.com/play-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a, https://github.com/play-with-docker/play-with-docker/security/advisories/GHSA-vq59-5x26-h639	A-PLA-PLAY-050423/989
Affected Version(s): 0.0.2					
Authorization Bypass	16-Mar-2023	6.5	Play With Docker is a browser-based Docker	https://github.com/pl	A-PLA-PLAY-050423/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Through User-Controlled Key			playground. Versions 0.0.2 and prior are vulnerable to domain hijacking. Because CORS configuration was not correct, an attacker could use `play-with-docker.com` as an example and set the origin header in an http request as `evil-play-with-docker.com`. The domain would echo in response header, which successfully bypassed the CORS policy and retrieved basic user information. This issue has been fixed in commit ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a. There are no known workarounds. **CVE ID : CVE-2023-28109**	ay-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a, https://github.com/play-with-docker/play-with-docker/security/advisories/GHSA-vq59-5x26-h639	
Vendor: Pluck-cms					
Product: pluck					
Affected Version(s): * Up to (excluding) 4.7.16					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	7.2	Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its “albums” module. Albums are used to create collections of images that can be inserted into web	https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/	A-PLU-PLUC-050423/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability. CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.2 High) **CVE ID : CVE-2023-25828**		
Affected Version(s): 4.7.16					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	7.2	Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its “albums” module. Albums are used to create collections of images that can be	https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/	A-PLU-PLUC-050423/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inserted into web pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability. CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.2 High) **CVE ID : CVE-2023-25828**		
Vendor: plugin					
Product: waiting					
Affected Version(s): * Up to (including) 0.6.2					
Improper Neutralization of Special Elements	22-Mar-2023	8.8	The Waiting: One-click Countdowns WordPress Plugin, version <= 0.6.2, is affected by an	N/A	A-PLU-WAIT-050423/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the pbc_down[meta][id] parameter of the pbc_save_downs action. **CVE ID : CVE-2023-28659**		
Vendor: pluginus					
Product: inpost_gallery					
Affected Version(s): * Up to (including) 2.1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The InPost Gallery WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'imgurl' parameter to the add_inpost_gallery_slide_item action, which can only be triggered by an authenticated user. **CVE ID : CVE-2023-28666**	N/A	A-PLU-INPO-050423/994
Product: wordpress_meta_data_and_taxonomies_filter					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The Meta Data and Taxonomies Filter WordPress plugin, in versions < 1.3.1, is affected by a reflected cross-site scripting vulnerability in the 'tax_name' parameter of the mdf_get_tax_options_in_widget action, which can only be triggered	N/A	A-PLU-WORD-050423/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by an authenticated user. **CVE ID : CVE-2023-28664**		
Vendor: Postgresql					
Product: pgadmin_4					
Affected Version(s): * Up to (excluding) 6.19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	6.5	pgAdmin 4 versions prior to v6.19 contains a directory traversal vulnerability. A user of the product may change another user's settings or alter the database. **CVE ID : CVE-2023-0241**	https://github.com/pgadmin-org/pgadmin4/issues/5734	A-POS-PGAD-050423/996
Vendor: Prestashop					
Product: eo_tags					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	The eo_tags package before 1.3.0 for PrestaShop allows SQL injection via an HTTP User-Agent or Referer header. **CVE ID : CVE-2023-27569**	N/A	A-PRE-EO_T-050423/997
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.4.19					
Improper Neutralization of Special Elements used in an SQL Command	21-Mar-2023	9.8	The eo_tags package before 1.4.19 for PrestaShop allows SQL injection via a crafted _ga cookie. **CVE ID : CVE-2023-27570**	https://security.profileo.com/cve/eo_tags_2023-27569-27570/	A-PRE-EO_T-050423/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Vendor: Qemu					
Product: qemu					
Affected Version(s): * Up to (including) 7.2.0					
Allocation of Resources Without Limits or Throttling	23-Mar-2023	5.5	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to allocate and initialize a huge number of page tables to be used as a ring of descriptors for CQ and async events, potentially leading to an out-of-bounds read and crash of QEMU. **CVE ID : CVE-2023-1544**	https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html, https://bugzilla.redhat.com/show_bug.cgi?id=2180364	A-QEM-QEMU-050423/999
Vendor: Qibosoft					
Product: qibocms					
Affected Version(s): v7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	8.8	Qibosoft QiboCMS v7 was discovered to contain a remote code execution (RCE) vulnerability via the Get_Title function at label_set_rs.php **CVE ID : CVE-2023-27037**	https://github.com/dienamer/vul/blob/main/2023-01-14.md	A-QIB-QIBO-050423/1000
Vendor: qykcms					
Product: qykcms					
Affected Version(s): 4.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	17-Mar-2023	7.2	A vulnerability was found in Meizhou Qingyunke QYKCMS 4.3.0. It has been classified as problematic. This affects an unknown part of the file /admin_system/api.php of the component Update Handler. The manipulation of the argument downurl leads to unrestricted upload. 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-223287. **CVE ID : CVE-2023-1442**	N/A	A-QYK-QYKC-050423/1001
Vendor: Radare					
Product: radare2					
Affected Version(s): * Up to (excluding) 5.8.6					
Uncontrolled Resource Consumption	23-Mar-2023	7.5	Denial of Service in GitHub repository radareorg/radare2 prior to 5.8.6. **CVE ID : CVE-2023-1605**	https://github.com/radareorg/radare2/commit/508a6307045441defd1bef0999a1f7052097613f, https://huntr.dev/bounties/9dddcf5b-7dd4-46cc-	A-RAD-RADA-050423/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				abf9-172dce20bab2	
Vendor: Rapid7					
Product: insightappsec					
Affected Version(s): * Up to (excluding) 23.2.1					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed getattr() method via a Jinja template to smuggle OS commands and perform other actions that are normally expected to be private methods. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. **CVE ID : CVE-2023-1304**	N/A	A-RAP-INSI-050423/1003
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed resource.db() accessor method to smuggle Python method calls via a Jinja template, which can lead to code execution. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed	N/A	A-RAP-INSI-050423/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of InsightCloudSec. **CVE ID : CVE-2023-1306**		
N/A	21-Mar-2023	8.1	An authenticated attacker can leverage an exposed "box" object to read and write arbitrary files from disk, provided those files can be parsed as yaml or JSON. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. **CVE ID : CVE-2023-1305**	N/A	A-RAP-INSI-050423/1005
Product: insightcloudsec					
Affected Version(s): * Up to (excluding) 2023.02.01					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed getattr() method via a Jinja template to smuggle OS commands and perform other actions that are normally expected to be private methods. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed	N/A	A-RAP-INSI-050423/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of InsightCloudSec. **CVE ID : CVE-2023-1304**		
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed resource.db() accessor method to smuggle Python method calls via a Jinja template, which can lead to code execution. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. **CVE ID : CVE-2023-1306**	N/A	A-RAP-INSI-050423/1007
N/A	21-Mar-2023	8.1	An authenticated attacker can leverage an exposed “box” object to read and write arbitrary files from disk, provided those files can be parsed as yaml or JSON. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. **CVE ID : CVE-2023-1305**	N/A	A-RAP-INSI-050423/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: insightvm					
Affected Version(s): * Up to (excluding) 6.6.179					
URL Redirection to Untrusted Site ('Open Redirect')	20-Mar-2023	6.1	Rapid7 InsightVM versions 6.6.178 and lower suffers from an open redirect vulnerability, whereby an attacker has the ability to redirect the user to a site of the attacker's choice using the 'page' parameter of the 'data/console/redirect' component of the application. This issue was resolved in the February, 2023 release of version 6.6.179. **CVE ID : CVE-2023-0681**	N/A	A-RAP-INSI-050423/1009
Vendor: rapidload					
Product: rapidload_power-up_for_autoptimize					
Affected Version(s): * Up to (excluding) 1.7.2					
Cross-Site Request Forgery (CSRF)	17-Mar-2023	6.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on its AJAX actions. This makes it possible for unauthenticated attackers to invoke those functions, via forged request	N/A	A-RAP-RAPI-050423/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			granted they can trick a site administrator into performing an action such as clicking on a link. Actions include resetting the API key, accessing or deleting log files, and deleting cache among others. **CVE ID : CVE-2023-1472**		
Vendor: react_webcam_project					
Product: react_webcam					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The React Webcam WordPress plugin through 1.2.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0365**	N/A	A-REA-REAC-050423/1011
Vendor: real.kit_project					
Product: real.kit					
Affected Version(s): * Up to (excluding) 5.1.1					
Improper Neutralization of Input During Web Page	20-Mar-2023	5.4	The real.Kit WordPress plugin before 5.1.1 does not validate and escape some of its shortcode attributes before	N/A	A-REA-REAL-050423/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0364**		
Vendor: really-simple-plugins					
Product: complianz					
Affected Version(s): * Up to (excluding) 6.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Complianz WordPress plugin before 6.4.2, Complianz Premium WordPress plugin before 6.4.2 do not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-1069**	N/A	A-REA-COMP-050423/1013
Vendor: redis					
Product: redis					
Affected Version(s): From (including) 7.0.8 Up to (excluding) 7.0.10					
Reachable Assertion	20-Mar-2023	5.5	Redis is an in-memory database that persists on disk. Starting in version 7.0.8 and prior	https://github.com/redis/redis/security/adv	A-RED-REDI-050423/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to version 7.0.10, authenticated users can use the MSETNX command to trigger a runtime assertion and termination of the Redis server process. The problem is fixed in Redis version 7.0.10. **CVE ID : CVE-2023-28425**	isories/GHSA-mvmm-4vq6-vw8c, https://github.com/redis/redis/commit/48e0d4788434833b47892fe9f3d91be7687f25c9	
Vendor: request_project					
Product: request					
Affected Version(s): * Up to (including) 2.88.1					
Server-Side Request Forgery (SSRF)	16-Mar-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** The Request package through 2.88.1 for Node.js allows a bypass of SSRF mitigations via an attacker-controller server that does a cross-protocol redirect (HTTP to HTTPS, or HTTPS to HTTP). NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-28155**	https://doyensec.com/resources/Doyensec_Advisory_RequestSSRF_Q12023.pdf, https://github.com/request/request/issues/3442, https://github.com/request/request/pull/3444	A-REQ-REQU-050423/1015
Vendor: responsive_hotel_site_project					
Product: responsive_hotel_site					
Affected Version(s): 1.0					
Improper Neutralization of	19-Mar-2023	9.8	A vulnerability classified as critical has been found in	N/A	A-RES-RESP-050423/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file messages.php of the component Newsletter Log Handler. The manipulation of the argument title 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-223398 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1498**		
Vendor: rifartek					
Product: iot_wall					
Affected Version(s): 22					
Incorrect Authorization	27-Mar-2023	8.1	RIFARTEK IOT Wall has a vulnerability of incorrect authorization. An authenticated remote attacker with general user privilege is allowed to perform specific privileged function to access and modify all sensitive data. **CVE ID : CVE-2023-25017**	https://www.twcert.org.tw/tw/cp-132-6962-34ac1-1.html	A-RIF-IOT_-050423/1017
Improper Neutralization of Input	27-Mar-2023	5.4	RIFARTEK IOT Wall transportation function has insufficient filtering	https://www.twcert.org.tw/tw/cp-132-6963-	A-RIF-IOT_-050423/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			for user input. An authenticated remote attacker with general user privilege can inject JavaScript to perform reflected XSS (Reflected Cross-site scripting) attack. **CVE ID : CVE-2023-25018**	7d2ee-1.html	
Vendor: rockoa					
Product: rockoa					
Affected Version(s): 2.3.2					
Unrestricted Upload of File with Dangerous Type	19-Mar-2023	8.8	A vulnerability, which was classified as critical, was found in RockOA 2.3.2. This affects the function runAction of the file acloudCosAction.php.SQL. The manipulation of the argument fileid leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223401 was assigned to this vulnerability. **CVE ID : CVE-2023-1501**	N/A	A-ROC-ROCK-050423/1019
Vendor: Rockwellautomation					
Product: modbus_tcp_server_add_on_instructions					
Affected Version(s): From (including) 2.00.00 Up to (excluding) 2.04.00					
Exposure of Sensitive Information to an	17-Mar-2023	4.3	Rockwell Automation Modbus TCP Server AOI prior to 2.04.00 is vulnerable to an	https://rockwellautomation.custhelp.com/ap	A-ROC-MODB-050423/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			unauthorized user sending a malformed message that could cause the controller to respond with a copy of the most recent response to the last valid request. If exploited, an unauthorized user could read the connected device's Modbus TCP Server AOI information. **CVE ID : CVE-2023-0027**	p/answers/answer_view/a_id/1138766	
Product: thinmanager					
Affected Version(s): 13.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27855		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1022
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. **CVE ID : CVE-2023-27857**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1023
Affected Version(s): 13.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1024
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.0.5					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. **CVE ID : CVE-2023-27857**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1026
Affected Version(s): From (including) 11.0.0 Up to (including) 11.0.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1028
Affected Version(s): From (including) 11.1.0 Up to (excluding) 11.1.5					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a read access violation. **CVE ID : CVE-2023-27857**		
Affected Version(s): From (including) 11.1.0 Up to (including) 11.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1030
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**		
Affected Version(s): From (including) 11.2.0 Up to (excluding) 11.2.6					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. **CVE ID : CVE-2023-27857**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1032
Affected Version(s): From (including) 11.2.0 Up to (including) 11.2.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1034
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.0.3					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. **CVE ID : CVE-2023-27857**		
Affected Version(s): From (including) 12.0.0 Up to (including) 12.0.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1036
Improper Limitation of a Pathname to a Restricted	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's	https://rockwellautomation.custhelp.com/app/answers/answer_vi	A-ROC-THIN-050423/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	ew/a_id/1138640	
Affected Version(s): From (including) 12.1.0 Up to (excluding) 12.1.4					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. **CVE ID : CVE-2023-27857**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1038
Affected Version(s): From (including) 12.1.0 Up to (including) 12.1.5					
Improper Limitation of a Pathname to a Restricted Directory	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An	https://rockwellautomation.custhelp.com/app/answers/answer_vi	A-ROC-THIN-050423/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**	ew/a_id/1138640	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1040
Affected Version(s): From (including) 6.0.0 Up to (including) 10.0.2					
Improper Limitation of a Pathname to a	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's	https://rockwellautomation.custhelp.com/app/answers	A-ROC-THIN-050423/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. **CVE ID : CVE-2023-27855**	/answer_view/a_id/1138640	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. **CVE ID : CVE-2023-27856**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640	A-ROC-THIN-050423/1042
Vendor: ruifang-tech					
Product: rebuild					
Affected Version(s): * Up to (including) 3.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Rebuild up to 3.2.3. Affected by this issue is some unknown functionality of the file /project/tasks/list. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-223742 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1610**	N/A	A-RUI-REBU-050423/1043
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in Rebuild up to 3.2.3. This affects an unknown part of the file /files/list-file. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of	https://github.com/getrebuild/rebuild/issues/598, https://vuldb.com/?id.223743, https://vuldb.com/?ctiid.223743	A-RUI-REBU-050423/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is VDB-223743. **CVE ID : CVE-2023-1612**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	8.8	A vulnerability classified as critical was found in Rebuild up to 3.2.3. Affected by this vulnerability is the function queryListOfConfig of the file /admin/robot/approval/list. The manipulation of the argument q leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is c9474f84e5f376dd2ade2078e3039961a9425da7. It is recommended to apply a patch to fix this issue. The identifier VDB-223381 was assigned to this vulnerability. **CVE ID : CVE-2023-1495**	https://github.com/getrebuild/rebuild/commit/c9474f84e5f376dd2ade2078e3039961a9425da7	A-RUI-REBU-050423/1045
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	A vulnerability has been found in Rebuild up to 3.2.3 and classified as problematic. This vulnerability affects unknown code of the file /feeds/post/publish.	N/A	A-RUI-REBU-050423/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-223744. **CVE ID : CVE-2023-1613**		
Vendor: russh_project					
Product: russh					
Affected Version(s): 0.37.0					
Improper Verification of Cryptographic Signature	16-Mar-2023	5.9	russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can lead to insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving peer are most likely to be problematic. These may vulnerable to eavesdropping. Most other	https://github.com/warp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg, https://github.com/warp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e	A-RUS-RUSS-050423/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementations reject such keys, so this is mainly an interoperability issue in such a case. This issue is fixed in versions 0.36.2 and 0.37.1 **CVE ID : CVE-2023-28113**		
Affected Version(s): From (including) 0.34.0 Up to (excluding) 0.36.2					
Improper Verification of Cryptographic Signature	16-Mar-2023	5.9	russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can lead to insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving peer are most likely to be problematic. These may vulnerable to eavesdropping. Most other implementations reject such keys, so this is mainly an interoperability issue in such a case. This issue is fixed in versions 0.36.2 and 0.37.1	https://github.com/warp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg, https://github.com/warp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e	A-RUS-RUSS-050423/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28113		
Vendor: saan					
Product: world_clock					
Affected Version(s): * Up to (including) 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Saan World Clock WordPress plugin through 1.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0145**	N/A	A-SAA-WORL-050423/1049
Vendor: saml_project					
Product: saml					
Affected Version(s): 0.4.12					
Allocation of Resources Without Limits or Throttling	22-Mar-2023	7.5	The crewjam/saml go library contains a partial implementation of the SAML standard in golang. Prior to version 0.4.13, the package's use of `flate.NewReader` does not limit the size of the input. The user can pass more than 1 MB of data in the HTTP request to the processing functions, which will be	https://github.com/crewjam/saml/commit/8e9236867d176ad6338c870a84e2039aef8a5021, https://github.com/crewjam/saml/security/advisories/GHSA-	A-SAM-SAML-050423/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decompressed server-side using the Deflate algorithm. Therefore, after repeating the same request multiple times, it is possible to achieve a reliable crash since the operating system kills the process. This issue is patched in version 0.4.13. **CVE ID : CVE-2023-28119**	5mqj-xc49-246p	
Vendor: Samsung					
Product: bixbytouch					
Affected Version(s): * Up to (excluding) 3.2.02.5					
N/A	16-Mar-2023	5.5	Improper access control vulnerability in BixbyTouch prior to version 3.2.02.5 in China models allows untrusted applications access local files. **CVE ID : CVE-2023-21465**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-BIXB-050423/1051
Product: calendar					
Affected Version(s): * Up to (excluding) 12.3.08.2000					
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. **CVE ID : CVE-2023-21464**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-CALE-050423/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 12.4.02.9000					
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. **CVE ID : CVE-2023-21464**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-CALE-050423/1053
Product: myfiles					
Affected Version(s): * Up to (excluding) 12.2.09.0					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. **CVE ID : CVE-2023-21463**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-MYFI-050423/1054
Affected Version(s): * Up to (excluding) 13.1.03.501					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-MYFI-050423/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. **CVE ID : CVE-2023-21463**		
Affected Version(s): * Up to (excluding) 14.1.03.0					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. **CVE ID : CVE-2023-21463**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-MYFI-050423/1056
Product: quick_share					
Affected Version(s): * Up to (excluding) 3.5.14.18					
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission.	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-QUIC-050423/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21462		
Affected Version(s): * Up to (excluding) 3.5.16.20					
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. **CVE ID : CVE-2023-21462**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	A-SAM-QUIC-050423/1058
Vendor: schedulicity					
Product: schedulicity					
Affected Version(s): * Up to (including) 2.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Schedulicity WordPress plugin through 2.21 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0491**	N/A	A-SCH-SCHE-050423/1059
Vendor: Schneider-electric					
Product: custom_reports					
Affected Version(s): * Up to (including) 16.0.0.23040					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-Mar-2023	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) **CVE ID : CVE-2023-27980**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1060
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27981**		
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27982**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1062
Improper Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that	https://download.schneider-electric.co	A-SCH-CUST-050423/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27984**	m/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.0.23040 and prior). **CVE ID : CVE-2023-27978**		
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27977**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1065
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, this could lead to denial of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+	A-SCH-CUST-050423/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27979**	Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Missing Authentication for Critical Function	21-Mar-2023	5.3	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27983**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-CUST-050423/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: igss_dashboard					
Affected Version(s): * Up to (including) 16.0.0.23040					
Missing Authentication for Critical Function	21-Mar-2023	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) **CVE ID : CVE-2023-27980**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1068
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEV	A-SCH-IGSS-050423/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27981**	D-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27982**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27984**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1071
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27978**		
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27977**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1073
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could allow the renaming of files in	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-	A-SCH-IGSS-050423/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the IGSS project report directory, this could lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27979**	04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Missing Authentication for Critical Function	21-Mar-2023	5.3	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.0.23040 and prior). **CVE ID : CVE-2023-27983**		
Product: igss_data_server					
Affected Version(s): * Up to (including) 16.0.0.23040					
Missing Authentication for Critical Function	21-Mar-2023	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) **CVE ID : CVE-2023-27980**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1076
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDo	A-SCH-IGSS-050423/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27981**	cType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.0.23040 and prior). **CVE ID : CVE-2023-27982**		
Improper Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27984**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1079
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEV	A-SCH-IGSS-050423/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27978**	D-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27977**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1081
Insufficient Verification of Data	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity	https://download.schneider-electric.co	A-SCH-IGSS-050423/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, this could lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27979**	m/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Missing Authentication for Critical Function	21-Mar-2023	5.3	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	A-SCH-IGSS-050423/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). **CVE ID : CVE-2023-27983**		
Vendor: school_registration_and_fee_system_project					
Product: school_registration_and_fee_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	School Registration and Fee System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at/bilal final/edit_user.php. **CVE ID : CVE-2023-27041**	https://github.com/forsean/bug_report/blob/main/vendors/hemedy99/School%20Registration%20and%20Fee%20System/SQLi-1.md	A-SCH-SCHO-050423/1084
Vendor: sentry					
Product: sentry_software_development_kit					
Affected Version(s): * Up to (excluding) 1.14.0					
Insertion of Sensitive Information Into Sent Data	22-Mar-2023	6.5	Sentry SDK is the official Python SDK for Sentry, real-time crash reporting software. When using the Django integration of versions prior to 1.14.0 of the Sentry SDK in a specific configuration it is possible to leak sensitive cookies values, including the session cookie to Sentry. These	https://github.com/getsentry/sentry-python/pull/1842, https://github.com/getsentry/sentry-python/security/advisories/GHSA-29pr-6jr8-q5jm	A-SEN-SENT-050423/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive cookies could then be used by someone with access to your Sentry issues to impersonate or escalate their privileges within your application. In order for these sensitive values to be leaked, the Sentry SDK configuration must have `sendDefaultPII` set to `True`; one must use a custom name for either `SESSION_COOKIE_NAME` or `CSRF_COOKIE_NAME` in one's Django settings; and one must not be configured in one's organization or project settings to use Sentry's data scrubbing features to account for the custom cookie names. As of version 1.14.0, the Django integration of the `sentry-sdk` will detect the custom cookie names based on one's Django settings and will remove the values from the payload before sending the data to Sentry. As a workaround, use the SDK's filtering mechanism to remove the cookies from the payload that is sent to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sentry. For error events, this can be done with the `before_send` callback method and for performance related events (transactions) one can use the `before_send_transaction` callback method. Those who want to handle filtering of these values on the server-side can also use Sentry's advanced data scrubbing feature to account for the custom cookie names. Look for the `$http.cookies`, `$http.headers`, `$request.cookies`, or `$request.headers` fields to target with a scrubbing rule. **CVE ID : CVE-2023-28117**		
Vendor: service_area_postcode_checker_project					
Product: service_area_postcode_checker					
Affected Version(s): * Up to (including) 2.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) vulnerability in Second2none Service Area Postcode Checker plugin <= 2.0.8 versions. **CVE ID : CVE-2023-25782**	N/A	A-SER-SERV-050423/1086
Vendor: silabs					
Product: wi-sun_software_development_kit					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.5.0					
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN SDK v1.5.0 and earlier allows malicious node to route malicious messages through network. **CVE ID : CVE-2023-1261**	N/A	A-SIL-WI-S-050423/1087
Vendor: Silverstripe					
Product: graphql					
Affected Version(s): 4.1.1					
Allocation of Resources Without Limits or Throttling	16-Mar-2023	7.5	`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execute a denial of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users should upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability. **CVE ID : CVE-2023-28104**	https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-67g8-c724-8mp3, https://github.com/silverstripe/silverstripe-graphql/releases/tag/4.1.2, https://github.com/silverstripe/silverstripe-graphql/pull/526	A-SIL-GRAP-050423/1088
Affected Version(s): 4.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	16-Mar-2023	7.5	`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execute a denial of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users should upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability. **CVE ID : CVE-2023-28104**	https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-67g8-c724-8mp3, https://github.com/silverstripe/silverstripe-graphql/releases/tag/4.1.2, https://github.com/silverstripe/silverstripe-graphql/pull/526	A-SIL-GRAP-050423/1089
Vendor: simplefilelist					
Product: simple_file_list					
Affected Version(s): * Up to (excluding) 6.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	The Simple File List WordPress plugin before 6.0.10 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	N/A	A-SIM-SIMP-050423/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disallowed (for example in multisite setup). **CVE ID : CVE-2023-1025**		
Vendor: simple_and_beautiful_shopping_cart_system_project					
Product: simple_and_beautiful_shopping_cart_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.8	A vulnerability classified as critical has been found in Simple and Beautiful Shopping Cart System 1.0. This affects an unknown part of the file uploadera.php. The manipulation leads to unrestricted upload. 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-223551. **CVE ID : CVE-2023-1558**	N/A	A-SIM-SIMP-050423/1091
Vendor: simple_and_nice_shopping_cart_script_project					
Product: simple_and_nice_shopping_cart_script					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	19-Mar-2023	9.8	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script 1.0. It has been rated as critical. This issue affects some unknown processing of the file	N/A	A-SIM-SIMP-050423/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploaderm.php. The manipulation of the argument submit leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223397 was assigned to this vulnerability. **CVE ID : CVE-2023-1497**		
Vendor: simple_art_gallery_project					
Product: simple_art_gallery					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	9.8	A vulnerability classified as critical was found in code-projects Simple Art Gallery 1.0. Affected by this vulnerability is an unknown functionality of the file adminHome.php. The manipulation of the argument reach_city 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-223399. **CVE ID : CVE-2023-1499**	N/A	A-SIM-SIMP-050423/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in code-projects Simple Art Gallery 1.0. Affected by this issue is some unknown functionality of the file adminHome.php. The manipulation of the argument about_info leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223400. **CVE ID : CVE-2023-1500**	N/A	A-SIM-SIMP-050423/1094
Vendor: simple_customer_relationship_management_system_project					
Product: simple_customer_relationship_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter under the Profile Update function. **CVE ID : CVE-2023-24655**	N/A	A-SIM-SIMP-050423/1095
Vendor: simple_image_gallery_web_app_project					
Product: simple_image_gallery_web_app					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Mar-2023	9.8	Simple Image Gallery v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the username parameter. **CVE ID : CVE-2023-27040**	N/A	A-SIM-SIMP-050423/1096
Vendor: simple_music_player_project					
Product: simple_music_player					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	18-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Simple Music Player 1.0. Affected is an unknown function of the file save_music.php. The manipulation of the argument filename leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223362 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1479**	N/A	A-SIM-SIMP-050423/1097
Vendor: simple_online_hotel_reservation_system_project					
Product: simple_online_hotel_reservation_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in code-projects Simple Online Hotel Reservation System 1.0. Affected is an unknown function of the file add_room.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. VDB-223554 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1561**	N/A	A-SIM-SIMP-050423/1098
Vendor: simplygallery					
Product: simply_gallery_blocks_with_lightbox					
Affected Version(s): * Up to (excluding) 3.0.8					
Missing Authorization	27-Mar-2023	8.1	The Gallery Blocks with Lightbox WordPress plugin before 3.0.8 has an AJAX endpoint that can be accessed by any authenticated users, such as subscriber. The callback function allows numerous actions, the most serious one being reading and updating the WordPress options which could be used to enable registration with a default administrator user role.	N/A	A-SIM-SIMP-050423/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0441		
Vendor: smplredirectionsmanager_project					
Product: smplredirectionsmanager					
Affected Version(s): * Up to (excluding) 1.1.19					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Mar-2023	9.8	SQL injection vulnerability found in PrestaShop smplredirectionsmanager v.1.1.19 and before allow a remote attacker to gain privileges via the SmplTools::getMatchingRedirectionsFromPartscomponent. **CVE ID : CVE-2023-26864**	https://friends-of-presta.github.io/security-advisories/modules/2023/01/17/smplredirectionsmanager.html	A-SMP-SMPL-050423/1100
Vendor: softmaker					
Product: flexipdf					
Affected Version(s): 2022					
Out-of-bounds Write	23-Mar-2023	7.8	A stack overfow in SoftMaker Software GmbH FlexiPDF v3.0.3.0 allows attackers to execute arbitrary code after opening a crafted PDF file. **CVE ID : CVE-2023-24295**	N/A	A-SOF-FLEX-050423/1101
Vendor: squidex.io					
Product: squidex					
Affected Version(s): * Up to (excluding) 7.4.0					
Improper Neutralization of Input During	18-Mar-2023	6.1	Squidex before 7.4.0 was discovered to contain a squid.svg cross-site scripting (XSS) vulnerability.	N/A	A-SQU-SQUI-050423/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-24278**		
Vendor: storage_unit_rental_management_system_project					
Product: storage_unit_rental_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	7.2	A vulnerability classified as problematic was found in SourceCodester Storage Unit Rental Management System 1.0. This vulnerability affects unknown code of the file classes/Users.php?f=save. The manipulation leads to unrestricted upload. 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-223552. **CVE ID : CVE-2023-1559**	N/A	A-STO-STOR-050423/1103
Vendor: strangerstudios					
Product: paid_memberships_pro					
Affected Version(s): * Up to (excluding) 2.9.12					
Improper Neutralization of Special Elements used in an SQL Command	20-Mar-2023	8.8	The Paid Memberships Pro WordPress plugin before 2.9.12 does not prevent subscribers from rendering shortcodes that concatenate attributes	N/A	A-STR-PAID-050423/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			directly into an SQL query. **CVE ID : CVE-2023-0631**		
Vendor: strategy11					
Product: formidable_form_builder					
Affected Version(s): * Up to (excluding) 6.1					
Authentication Bypass by Spoofing	27-Mar-2023	6.5	The Formidable Forms WordPress plugin before 6.1 uses several potentially untrusted headers to determine the IP address of the client, leading to IP Address spoofing and bypass of anti-spam protections. **CVE ID : CVE-2023-0816**	N/A	A-STR-FORM-050423/1105
Vendor: streamlit					
Product: streamlit					
Affected Version(s): From (including) 0.63.0 Up to (excluding) 0.81.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	6.1	Streamlit, software for turning data scripts into web applications, had a cross-site scripting (XSS) vulnerability in versions 0.63.0 through 0.80.0. Users of hosted Streamlit app(s) were vulnerable to a reflected XSS vulnerability. An attacker could craft a malicious URL with Javascript payloads to a Streamlit app. The attacker could then trick the user into	https://github.com/streamlit/streamlit/security/advisories/GHSA-9c6g-qpgj-rvxw, https://github.com/streamlit/streamlit/commit/afcf880c60e5d7538936cc2d9721b9e1bc02b075	A-STR-STRE-050423/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visiting the malicious URL and, if successful, the server would render the malicious javascript payload as-is, leading to XSS. Version 0.81.0 contains a patch for this vulnerability. **CVE ID : CVE-2023-27494**		
Vendor: student_study_center_desk_management_system_project					
Product: student_study_center_desk_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0. It has been rated as critical. This issue affects the function view_student of the file admin/?page=students/view_student. The manipulation of the argument id with the input 3' AND (SELECT 2100 FROM (SELECT(SLEEP(5)))FWlC) AND 'butz'='butz 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-223325 was assigned to this vulnerability.	N/A	A-STU-STUD-050423/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1466		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file Master.php?f=delete_img of the component POST Parameter Handler. The manipulation of the argument path with the input C%3A%2Ffoo.txt leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223326 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1467**	N/A	A-STU-STUD-050423/1108
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=reports&date_from=2023-02-17&date_to=2023-03-	N/A	A-STU-STUD-050423/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17 of the component Report Handler. The manipulation of the argument date_from/date_to leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-223327. **CVE ID : CVE-2023-1468**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/assign/assign.php. The manipulation of the argument id 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-223555. **CVE ID : CVE-2023-1563**	N/A	A-STU-STUD-050423/1110
Improper Neutralization of	22-Mar-2023	6.1	A vulnerability was found in SourceCodester	N/A	A-STU-STUD-050423/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Student Study Center Desk Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/assign/assign.php. The manipulation of the argument sid 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-223559. **CVE ID : CVE-2023-1567**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A vulnerability classified as problematic has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file /admin/reports/index.php of the component GET Parameter Handler. The manipulation of the argument date_to leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to	N/A	A-STU-STUD-050423/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier of this vulnerability is VDB-223560. **CVE ID : CVE-2023-1568**		
Vendor: sudo_project					
Product: sudo					
Affected Version(s): * Up to (excluding) 1.9.13					
Improper Encoding or Escaping of Output	16-Mar-2023	5.3	Sudo before 1.9.13 does not escape control characters in log messages. **CVE ID : CVE-2023-28486**	https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca	A-SUD-SUDO-050423/1113
Improper Encoding or Escaping of Output	16-Mar-2023	5.3	Sudo before 1.9.13 does not escape control characters in sudoreplay output. **CVE ID : CVE-2023-28487**	https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca	A-SUD-SUDO-050423/1114
Vendor: superior_faq_project					
Product: superior_faq					
Affected Version(s): * Up to (including) 1.0.2					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Rafael Dery Superior FAQ plugin <= 1.0.2 versions. **CVE ID : CVE-2023-22678**	N/A	A-SUP-SUPE-050423/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Swftools					
Product: swftools					
Affected Version(s): 0.9.2					
Out-of-bounds Write	23-Mar-2023	5.5	swfdump v0.9.2 was discovered to contain a heap buffer overflow in the function swf_GetPlaceObject at swfobject.c. **CVE ID : CVE-2023-27249**	N/A	A-SWF-SWFT-050423/1116
Vendor: tailscale					
Product: tailscale					
Affected Version(s): From (including) 1.34 Up to (excluding) 1.38.2					
Improper Privilege Management	23-Mar-2023	8	Tailscale is software for using Wireguard and multi-factor authentication (MFA). A vulnerability identified in the implementation of Tailscale SSH starting in version 1.34.0 and prior to prior to 1.38.2 in FreeBSD allows commands to be run with a higher privilege group ID than that specified in Tailscale SSH access rules. A difference in the behavior of the FreeBSD `setgroups` system call from POSIX meant that the Tailscale client running on a FreeBSD-based operating system did not appropriately restrict groups on the host	https://github.com/tailscale/tailscale/releases/tag/v1.38.2, https://tailscale.com/security-bulletins/#ts-2023-003, https://github.com/tailscale/tailscale/commit/d00c046b723dff6e3775d7d35f891403ac21a47d	A-TAI-TAIL-050423/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when using Tailscale SSH. When accessing a FreeBSD host over Tailscale SSH, the egid of the tailscaled process was used instead of that of the user specified in Tailscale SSH access rules. Tailscale SSH commands may have been run with a higher privilege group ID than that specified in Tailscale SSH access rules if they met all of the following criteria: the destination node was a FreeBSD device with Tailscale SSH enabled; Tailscale SSH access rules permitted access for non-root users; and a non-interactive SSH session was used. Affected users should upgrade to version 1.38.2 to remediate the issue. **CVE ID : CVE-2023-28436**		
Vendor: task_allocation_system_project					
Product: task_allocation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	29-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Simple Task Allocation System 1.0. Affected is	N/A	A-TAS-TASK-050423/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an unknown function of the file LoginRegistration.php?a=register_user. The manipulation of the argument Fullname leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-224244. **CVE ID : CVE-2023-1687**		
Vendor: teachpress_project					
Product: teachpress					
Affected Version(s): * Up to (excluding) 8.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in Michael Winkler teachPress plugin <= 8.1.8 versions. **CVE ID : CVE-2023-22704**	N/A	A-TEA-TEAC-050423/1119
Vendor: teacms_project					
Product: teacms					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-2023	9.8	A vulnerability has been found in XiaoBingBy TeaCMS up to 2.0.2 and classified as critical. This vulnerability affects unknown code of the file /admin/getallarticleinfo. The manipulation of the argument	N/A	A-TEA-TEAC-050423/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			searchInfo leads to sql injection. The attack can be initiated remotely. VDB-223366 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1483**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	5.4	A vulnerability was found in XiaoBingBy TeaCMS up to 2.0.2. It has been classified as problematic. Affected is an unknown function of the component Article Title Handler. The manipulation with the input <script>alert(document.cookie)</script> 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-223800. **CVE ID : CVE-2023-1616**	N/A	A-TEA-TEAC-050423/1121
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.0.23					
Improper Neutralization of Special Elements used in an	21-Mar-2023	7.5	SQL Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.0.23.	https://huntr.dev/bounties/942c015f-7486-49b1-94ae-	A-TEA-TEAM-050423/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2023-1545**	b1538d812bc2, https://github.com/nilsteampassnet/teampass/commit/4780252fdb600ef2ec2758f17a37d738570cbe66	
Authorization Bypass Through User-Controlled Key	17-Mar-2023	5.4	Improper Authorization in GitHub repository nilsteampassnet/teampass prior to 3.0.0.23. **CVE ID : CVE-2023-1463**	https://huntr.dev/bounties/f6683c3b-a0f2-4615-b639-1920c8ae12e6, https://github.com/nilsteampassnet/teampass/commit/4e06fbaf2b78c3615d0599855a72ba7e31157516	A-TEA-TEAM-050423/1123
Vendor: technocrackers					
Product: bulk_price_update_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The Woo Bulk Price Update WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'page' parameter to the techno_get_products	N/A	A-TEC-BULK-050423/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action, which can only be triggered by an authenticated user. **CVE ID : CVE-2023-28665**		
Vendor: temenos					
Product: t24					
Affected Version(s): r20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Temenos T24 Release 20 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the routineName parameter at genrequest.jsp. **CVE ID : CVE-2023-24367**	N/A	A-TEM-T24-050423/1125
Vendor: templatesnext					
Product: templatesnext_toolkit					
Affected Version(s): * Up to (excluding) 3.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TemplatesNext TemplatesNext ToolKit plugin <= 3.2.7 versions. **CVE ID : CVE-2023-22712**	N/A	A-TEM-TEMP-050423/1126
Vendor: tinydng_project					
Product: tinydng					
Affected Version(s): * Up to (excluding) 2023-02-20					
Heap-based Buffer Overflow	22-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in syoyo tinydng. Affected by	https://github.com/syoyo/tinydng/issues/29,	A-TIN-TINY-050423/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue is the function __interceptor_memcpy of the file tiny_dng_loader.h. The manipulation leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. It is recommended to apply a patch to fix this issue. VDB-223562 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1570**	https://github.com/syoyo/tinydng/issues/28	
Vendor: tinytiff_project					
Product: tinytiff					
Affected Version(s): 3.0.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in TinyTIFF 3.0.0.0. This issue affects some unknown processing of the file tinytiffreader.c of the component File Handler. The manipulation leads to	N/A	A-TIN-TINY-050423/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-223553 was assigned to this vulnerability. **CVE ID : CVE-2023-1560**		
Vendor: Tipsandtricks-hq					
Product: wordpress_simple_paypal_shopping_cart					
Affected Version(s): * Up to (including) 4.6.3					
Exposure of Sensitive Information to an Unauthorized Actor	16-Mar-2023	5.3	The WP Simple Shopping Cart plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.6.3 due to the plugin saving shopping cart data exports in a publicly accessible location (/wp-content/plugins/wordpress-simple-paypal-shopping-cart/includes/admin/). This makes it possible for unauthenticated attackers to view information that should be limited to administrators only and can include data like first name, last name, email, address, IP Address, and more.	N/A	A-TIP-WORD-050423/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1431		
Product: wp_express_checkout					
Affected Version(s): * Up to (excluding) 2.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	4.8	The WP Express Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pec_coupon[code]' parameter in versions up to, and including, 2.2.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrator-level access to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note: This can potentially be exploited by lower-privileged users if the `Admin Dashboard Access Permission` setting it set for those users to access the dashboard. **CVE ID : CVE-2023-1469**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2879453%40wp-express-checkout&new=2879453%40wp-express-checkout&sfp_email=&sfph_mail=	A-TIP-WP_E-050423/1130
Vendor: top_10_-_popular_posts_project					
Product: top_10_-_popular_posts					
Affected Version(s): * Up to (including) 3.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ajay D'Souza Top 10 – Popular posts plugin for WordPress plugin <= 3.2.4 versions. **CVE ID : CVE-2023-26008**	N/A	A-TOP-TOP_-050423/1131
Vendor: tosec					
Product: kirin_fortress_machine					
Affected Version(s): 1.7-2020-0610					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	SQL Injection vulnerability found in Kirin Fortress Machine v.1.7-2020-0610 allows attackers to execute arbitrary code via the /admin.php?controller=admin_commonuser parameter. **CVE ID : CVE-2023-26784**	N/A	A-TOS-KIRI-050423/1132
Vendor: Trendmicro					
Product: trend_micro_endpoint_encryption					
Affected Version(s): * Up to (including) 6.0.0.3204					
N/A	22-Mar-2023	6.8	A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows? Secure Boot process in an attempt to execute other attacks to obtain access to the contents	https://success.trendmicro.com/solution/000292473	A-TRE-TREN-050423/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone. **CVE ID : CVE-2023-28005**		
Product: txone_stellarone					
Affected Version(s): * Up to (excluding) 2.0.1160					
N/A	22-Mar-2023	8.8	TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must first obtain a low-privileged authenticated user's profile on the target system in order to	https://success.trendmicro.com/solution/000292486	A-TRE-TXON-050423/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability. **CVE ID : CVE-2023-25069**		
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails **CVE ID : CVE-2023-22288**	https://checkmk.com/werk/15069	A-TRI-CHEC-050423/1135
Affected Version(s): 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails **CVE ID : CVE-2023-22288**	https://checkmk.com/werk/15069	A-TRI-CHEC-050423/1136
Affected Version(s): From (including) 1.6.0 Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails	https://checkmk.com/werk/15069	A-TRI-CHEC-050423/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22288		
Vendor: trudesk_project					
Product: trudesk					
Affected Version(s): 1.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	5.4	Trudesk v1.2.6 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Tags parameter under the Create Ticket function. **CVE ID : CVE-2023-26982**	N/A	A-TRU-TRUD-050423/1138
Vendor: tshirtecommerce					
Product: tshirtecommerce					
Affected Version(s): 2.1.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised product_id GET parameter in order to exploit an insecure parameter in the front controller file designer.php, which could lead to a SQL injection. This is exploited in the wild in March 2023. **CVE ID : CVE-2023-27637**	https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html	A-TSH-TSHI-050423/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised tshirtecommerce_design_cart_id GET parameter in order to exploit an insecure parameter in the functions hookActionCartSave and updateCustomizationTable, which could lead to a SQL injection. This is exploited in the wild in March 2023. **CVE ID : CVE-2023-27638**	https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html	A-TSH-TSHI-050423/1140
Vendor: typecho					
Product: typecho					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via an arbitrarily supplied URL parameter. **CVE ID : CVE-2023-27130**	https://github.com/typecho/typecho/commit/f9ede542c9052ba22a6096d8412e2f02d9de872b	A-TYP-TYPE-050423/1141
Improper Neutralization of Input During	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code	N/A	A-TYP-TYPE-050423/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			viathe Post Editorparameter. **CVE ID : CVE-2023-27131**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via the Comment Manager /admin/manage-comments.php component. **CVE ID : CVE-2023-27711**	N/A	A-TYP-TYPE-050423/1143
Vendor: university_information_management_system_project					
Product: university_information_management_system					
Affected Version(s): * Up to (excluding) 23.03.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Izmir Katip Celebi University UBYS allows Stored XSS.This issue affects UBYS: before 23.03.16. **CVE ID : CVE-2023-0320**	N/A	A-UNI-UNIV-050423/1144
Vendor: utarit					
Product: persolus					
Affected Version(s): * Up to (excluding) 2.03.93					
Improper Neutralization of Special Elements	17-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	N/A	A-UTA-PERS-050423/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerability in Utarit Information Technologies Persolus allows SQL Injection. This issue affects Persolus: before 2.03.93. **CVE ID : CVE-2023-1152**		
Vendor: vadi					
Product: digikent					
Affected Version(s): * Up to (excluding) 23.03.20					
Authorization Bypass Through User-Controlled Key	21-Mar-2023	8.8	Authorization Bypass Through User-Controlled Key vulnerability in Vadi Corporate Information Systems DigiKent allows Authentication Bypass, Authentication Abuse. This issue affects DigiKent: before 23.03.20. **CVE ID : CVE-2023-1462**	N/A	A-VAD-DIGI-050423/1146
Vendor: vektor-inc					
Product: vk_all_in_one_expansion_unit					
Affected Version(s): * Up to (excluding) 9.87.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	The VK All in One Expansion Unit WordPress plugin before 9.87.1.0 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site	N/A	A-VEK-VK_A-050423/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Scripting in old web browsers **CVE ID : CVE-2023-0937**		
Vendor: Veritas					
Product: aptare_it_analytics					
Affected Version(s): * Up to (excluding) 10.6.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be downloaded and installed on collectors. **CVE ID : CVE-2023-28818**	https://www.veritas.com/content/support/en_US/security/VTS23-002	A-VER-APTA-050423/1148
Product: netbackup					
Affected Version(s): * Up to (excluding) 10.0					
Uncontrolled Search Path Element	23-Mar-2023	7.8	An issue was discovered in Veritas NetBackup before 10.0. A vulnerability in the way NetBackup validates the path to a DLL prior to loading may allow a lower level user to elevate	https://www.veritas.com/content/support/en_US/security/VTS22-010#M2	A-VER-NETB-050423/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges and compromise the system. **CVE ID : CVE-2023-28759**		
Affected Version(s): * Up to (excluding) 8.3.0.2					
N/A	23-Mar-2023	7.1	An issue was discovered in Veritas NetBackup before 8.3.0.2. BPCD allows an unprivileged user to specify a log file path when executing a NetBackup command. This can be used to overwrite existing NetBackup log files. **CVE ID : CVE-2023-28758**	https://www.veritas.com/content/support/en_US/security/VTS23-003	A-VER-NETB-050423/1150
Product: netbackup_it_analytics					
Affected Version(s): 11.0.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be	https://www.veritas.com/content/support/en_US/security/VTS23-002	A-VER-NETB-050423/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downloaded and installed on collectors. **CVE ID : CVE-2023-28818**		
Affected Version(s): 11.1.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be downloaded and installed on collectors. **CVE ID : CVE-2023-28818**	https://www.veritas.com/content/support/en_US/security/VTS23-002	A-VER-NETB-050423/1152
Vendor: veronalabs					
Product: wp_statistics					
Affected Version(s): * Up to (excluding) 14.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	8.8	The WP Statistics WordPress plugin before 14.0 does not escape a parameter, which could allow authenticated users to perform SQL Injection attacks. By default, the affected feature is available to users with	N/A	A-VER-WP_S-050423/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the manage_options capability (admin+), however the plugin has a settings to allow low privilege users to access it as well. **CVE ID : CVE-2023-0955**		
Vendor: versionize_project					
Product: versionize					
Affected Version(s): From (including) 0.1.1 Up to (excluding) 0.1.10					
Out-of-bounds Read	24-Mar-2023	7.5	Versionize is a framework for version tolerant serializion/deserialization of Rust data structures, designed for usecases that need fast deserialization times and minimal size overhead. An issue was discovered in the 'Versionize::deserialize' implementation provided by the 'versionize' crate for 'vmm_sys_utils::fam::FamStructWrapper', which can lead to out of bounds memory accesses. The impact started with version 0.1.1. The issue was corrected in version 0.1.10 by inserting a check that verifies, for any deserialized header, the lengths of compared flexible arrays are equal and aborting	https://github.com/firecracker-microvm/versionize/commit/a57a051ba006cfa3b41a0532f484df759e008d47	A-VER-VERS-050423/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deserialization otherwise. **CVE ID : CVE-2023-28448**		
Vendor: very_simple_google_maps_project					
Product: very_simple_google_maps					
Affected Version(s): * Up to (excluding) 2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Michael Aronoff Very Simple Google Maps plugin <= 2.8.4 versions. **CVE ID : CVE-2023-23864**	N/A	A-VER-VERY-050423/1155
Vendor: Vmware					
Product: spring_cloud_config					
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.6					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1156
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.1					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**		
Product: spring_cloud_vault					
Affected Version(s): 4.0.0					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1158
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.2					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1159
Product: spring_framework					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 5.2.22					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition. **CVE ID : CVE-2023-20861**	https://spring.io/security/cve-2023-20861	A-VMW-SPRI-050423/1160
Affected Version(s): From (including) 5.3.0 Up to (including) 5.3.25					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition. **CVE ID : CVE-2023-20861**	https://spring.io/security/cve-2023-20861	A-VMW-SPRI-050423/1161
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.6					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL	https://spring.io/security/cve-2023-20861	A-VMW-SPRI-050423/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expression that may cause a denial-of-service (DoS) condition. **CVE ID : CVE-2023-20861**		
Product: spring_vault					
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.3					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1163
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.2					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. **CVE ID : CVE-2023-20859**	https://spring.io/security/cve-2023-20859	A-VMW-SPRI-050423/1164
Vendor: vox2mesh_project					
Product: vox2mesh					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-Mar-2023	5.5	vox2mesh 1.0 has stack-overflow in main.cpp, this is stack-overflow caused by incorrect use of memcpy() funciton. The flow allows an attacker to cause a denial of service (abort) via a crafted file. **CVE ID : CVE-2023-27754**	N/A	A-VOX-VOX2-050423/1165
Vendor: vxsearch					
Product: vx_search					
Affected Version(s): 13.8					
Unquoted Search Path or Element	16-Mar-2023	7.8	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file. **CVE ID : CVE-2023-24671**	N/A	A-VXS-VX_S-050423/1166
Affected Version(s): 14.7					
Unquoted Search Path or Element	16-Mar-2023	7.8	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file. **CVE ID : CVE-2023-24671**	N/A	A-VXS-VX_S-050423/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: watchdog					
Product: anti-virus					
Affected Version(s): 1.4.214.0					
Improper Access Control	17-Mar-2023	7.1	A vulnerability was found in Watchdog Anti-Virus 1.4.214.0. It has been rated as critical. Affected by this issue is the function 0x80002008 in the library wsdk-driver.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-223298 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1453**	N/A	A-WAT-ANTI-050423/1168
NULL Pointer Dereference	17-Mar-2023	5.5	A vulnerability classified as problematic was found in Watchdog Anti-Virus 1.4.214.0. Affected by this vulnerability is the function 0x80002004/0x80002008 in the library wsdk-driver.sys of the component IoControlCode Handler. The	N/A	A-WAT-ANTI-050423/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223291. **CVE ID : CVE-2023-1446**		
Vendor: water_billing_system_project					
Product: water_billing_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	SourceCodester Water Billing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the lastname text box under the Add Client module. **CVE ID : CVE-2023-27241**	https://github.com/kaikai-11/WaterBilling-System, https://github.com/kaikai-11/WaterBilling-System/blob/main/README.md	A-WAT-WATE-050423/1170
Vendor: webnus					
Product: modern_events_calendar_lite					
Affected Version(s): * Up to (including) 5.16.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	The Modern Events Calendar Lite WordPress plugin through 5.16.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to	N/A	A-WEB-MODE-050423/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-1400**		
Vendor: westerndigital					
Product: sandisk_privateaccess					
Affected Version(s): * Up to (excluding) 6.4.9					
Use of a Broken or Risky Cryptographic Algorithm	24-Mar-2023	7.4	SanDisk PrivateAccess versions prior to 6.4.9 support insecure TLS 1.0 and TLS 1.1 protocols which are susceptible to man-in-the-middle attacks thereby compromising confidentiality and integrity of data. **CVE ID : CVE-2023-22812**	https://www.westerndigital.com/support/product-security/wdc-23005-sandisk-privateaccess-software-update	A-WES-SAND-050423/1172
Vendor: winwar					
Product: wp_ebay_product_feeds					
Affected Version(s): * Up to (excluding) 3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP eBay Product Feeds plugin <= 3.3.1 versions. **CVE ID : CVE-2023-23722**	N/A	A-WIN-WP_E-050423/1173
Product: wp_flipclock					
Affected Version(s): * Up to (excluding) 1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Flipclock plugin <= 1.7.4 versions. **CVE ID : CVE-2023-23728**	N/A	A-WIN-WP_F-050423/1174
Vendor: wisdomgarden					
Product: tronclass_ilearn					
Affected Version(s): 2.3.2					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	WisdomGarden Tronclass has improper access control when uploading file. An authenticated remote attacker with general user privilege can exploit this vulnerability to access files belonging to other users by modifying the file ID within URL. **CVE ID : CVE-2023-24834**	https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html	A-WIS-TRON-050423/1175
Affected Version(s): * Up to (excluding) 1.52.29198					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	WisdomGarden Tronclass has improper access control when uploading file. An authenticated remote attacker with general user privilege can exploit this vulnerability to access files belonging to other users by	https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html	A-WIS-TRON-050423/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the file ID within URL. **CVE ID : CVE-2023-24834**		
Vendor: wisecleaner					
Product: wise_force_deleter					
Affected Version(s): 1.5.3.54					
Improper Access Control	18-Mar-2023	7.1	A vulnerability classified as problematic was found in Lespeed WiseCleaner Wise Force Deleter 1.5.3.54. This vulnerability affects the function 0x220004 in the library WiseUnlock64.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223372. **CVE ID : CVE-2023-1486**	N/A	A-WIS-WISE-050423/1177
Product: wise_system_monitor					
Affected Version(s): 1.5.3.54					
Improper Access Control	18-Mar-2023	7.8	A vulnerability has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54 and classified	N/A	A-WIS-WISE-050423/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as critical. Affected by this vulnerability is the function 0x9C402088 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223375. **CVE ID : CVE-2023-1489**		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. This issue affects the function 0x9C40208C/0x9C402000/0x9C402084/0x9C402088/0x9C402004/0x9C4060C4/0x9C4060CC/0x9C4060D0/0x9C4060D4/0x9C40A0DC/0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The	N/A	A-WIS-WISE-050423/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-223373 was assigned to this vulnerability. **CVE ID : CVE-2023-1487**		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	A vulnerability, which was classified as problematic, was found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. Affected is the function 0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-223374 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1488**	N/A	A-WIS-WISE-050423/1180
Vendor: woocommerce_multiple_customer_addresses_\&_shipping_project					
Product: woocommerce_multiple_customer_addresses_\&_shipping					
Affected Version(s): * Up to (excluding) 21.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	20-Mar-2023	8.8	The WooCommerce Multiple Customer Addresses & Shipping WordPress plugin before 21.7 does not ensure that the address to add/update/retrieve/delete and duplicate belong to the user making the request, or is from a high privilege users, allowing any authenticated users, such as subscriber to add/update/duplicate/delete as well as retrieve addresses of other users. **CVE ID : CVE-2023-0865**	N/A	A-WOO-WOOC-050423/1181
Vendor: wp-commentnavi_project					
Product: wp-commentnavi					
Affected Version(s): * Up to (excluding) 1.12.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Lester 'GaMerZ' Chan WP-CommentNavi plugin <= 1.12.1 versions. **CVE ID : CVE-2023-22715**	N/A	A-WP--WP-C-050423/1182
Vendor: wp-master					
Product: feed_changer_\&_remover					
Affected Version(s): * Up to (including) 0.2					
Improper Neutralization of Input	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in WP-master.Ir Feed	N/A	A-WP--FEED-050423/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Changer & Remover plugin <= 0.2 versions. **CVE ID : CVE-2023-25795**		
Vendor: wp-slimstat					
Product: slimstat_analytics					
Affected Version(s): * Up to (excluding) 4.9.3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	8.8	The Slimstat Analytics WordPress plugin before 4.9.3.3 does not prevent subscribers from rendering shortcodes that concatenates attributes directly into an SQL query. **CVE ID : CVE-2023-0630**	N/A	A-WP--SLIM-050423/1184
Vendor: wpbean					
Product: wpb_advanced_faq					
Affected Version(s): * Up to (excluding) 1.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The WPB Advanced FAQ WordPress plugin through 1.0.6 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0370**	N/A	A-WPB-WPB_-050423/1185
Vendor: wpmobile.app_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wpmobile.app					
Affected Version(s): * Up to (excluding) 11.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WPMobile.App WPMobile.App — Android and iOS Mobile Application plugin <= 11.13 versions. **CVE ID : CVE-2023-22702**	N/A	A-WPM-WPMO-050423/1186
Vendor: wppool					
Product: wp_dark_mode					
Affected Version(s): * Up to (excluding) 4.0.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	4.3	The WP Dark Mode WordPress plugin before 4.0.8 does not properly sanitize the style parameter in shortcodes before using it to load a PHP template. This leads to Local File Inclusion on servers where non-existent directories may be traversed, or when chained with another vulnerability allowing arbitrary directory creation. **CVE ID : CVE-2023-0467**	N/A	A-WPP-WP_D-050423/1187
Vendor: wpvar					
Product: wp_shamsi					
Affected Version(s): * Up to (including) 4.3.3					
Cross-Site Request	27-Mar-2023	6.5	The WP Shamsi WordPress plugin through 4.3.3 has	N/A	A-WPV-WP_S-050423/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			CSRF and broken access control vulnerabilities which leads user with role as low as subscriber delete attachment. **CVE ID : CVE-2023-0335**		
Vendor: wp_better_emails_project					
Product: wp_better_emails					
Affected Version(s): * Up to (including) 0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nicolas Lemoine WP Better Emails plugin <= 0.4 versions. **CVE ID : CVE-2023-22679**	N/A	A-WP_-WP_B-050423/1189
Vendor: wp_htpasswd_project					
Product: wp_htpasswd					
Affected Version(s): * Up to (including) 1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Matteo Candura WP htpasswd plugin <= 1.7 versions. **CVE ID : CVE-2023-25064**	N/A	A-WP_-WP_H-050423/1190
Vendor: wp_image_carousel_project					
Product: wp_image_carousel					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input	27-Mar-2023	5.4	The WP Image Carousel WordPress plugin through 1.0.2 does not sanitise and	N/A	A-WP_-WP_I-050423/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some parameters, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks. **CVE ID : CVE-2023-0589**		
Vendor: wp_popup_banners_project					
Product: wp_popup_banners					
Affected Version(s): * Up to (including) 1.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	6.5	The WP Popup Banners plugin for WordPress is vulnerable to SQL Injection via the 'banner_id' parameter in versions up to, and including, 1.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with minimal permissions, such as a subscrber, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-1471**	N/A	A-WP_-WP_P-050423/1192
Vendor: X.org					
Product: x_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 21.1.7					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	A-X.O-X_SE-050423/1193
Vendor: xipblog_project					
Product: xipblog					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	9.8	SQL injection vulnerability found in PrestaShop xipblog v.2.0.1 and before allow a remote attacker to gain privileges via the xipcategoryclass and xippostsclass components. **CVE ID : CVE-2023-27847**	N/A	A-XIP-XIPB-050423/1194
Vendor: xpdfreader					
Product: xpdf					
Affected Version(s): 4.04					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.5	xpdf v4.04 was discovered to contain a stack overflow in the component pdftotext. **CVE ID : CVE-2023-27655**	https://forum.xpdfreader.com/viewtopic.php?t=42398	A-XPD-XPDF-050423/1195
Vendor: xuxueli					
Product: xxl-job					
Affected Version(s): 2.2.0					
N/A	21-Mar-2023	7.5	Permissions vulnerabiltiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter. **CVE ID : CVE-2023-27087**	N/A	A-XUX-XXL--050423/1196
Affected Version(s): 2.3.0					
N/A	21-Mar-2023	7.5	Permissions vulnerabiltiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter. **CVE ID : CVE-2023-27087**	N/A	A-XUX-XXL--050423/1197
Affected Version(s): 2.3.1					
N/A	21-Mar-2023	7.5	Permissions vulnerabiltiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter.	N/A	A-XUX-XXL--050423/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27087		
Vendor: xzjie_cms_project					
Product: xzjie_cms					
Affected Version(s): * Up to (including) 1.0.3					
Unrestricted Upload of File with Dangerous Type	18-Mar-2023	9.8	A vulnerability was found in xzjie cms up to 1.0.3 and classified as critical. This issue affects some unknown processing of the file /api/upload. The manipulation of the argument uploadFile leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-223367. **CVE ID : CVE-2023-1484**	https://gitee.com/xzjie/cms/issues/I6INIT	A-XZJ-XZJI-050423/1199
Vendor: young_entrepreneur_e-negosyo_system_project					
Product: young_entrepreneur_e-negosyo_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file /bsenordering/index.php of the component GET Parameter Handler. The manipulation of the	N/A	A-YOU-YOUN-050423/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument category with the input <script>alert(222)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223371. **CVE ID : CVE-2023-1485**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	A vulnerability was found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file bsenordering/admin/category/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert(233)</script> 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-224243.	N/A	A-YOU-YOUN-050423/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1686		
Vendor: Zoom					
Product: meetings					
Affected Version(s): * Up to (excluding) 5.13.5					
N/A	16-Mar-2023	7.8	Zoom Client for IT Admin Windows installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain during the installation process to escalate their privileges to the SYSTEM user. **CVE ID : CVE-2023-22883**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-MEET-050423/1202
Product: rooms					
Affected Version(s): * Up to (excluding) 5.13.3					
N/A	16-Mar-2023	7.5	Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-050423/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. **CVE ID : CVE-2023-22880**		
Product: virtual_desktop_infrastructure					
Affected Version(s): * Up to (excluding) 5.13.1					
N/A	16-Mar-2023	7.5	Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIRT-050423/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. **CVE ID : CVE-2023-22880**		
Product: zoom					
Affected Version(s): * Up to (excluding) 5.13.5					
N/A	16-Mar-2023	7.5	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely cause the client to crash, causing a denial of service. **CVE ID : CVE-2023-22881**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-050423/1205
N/A	16-Mar-2023	7.5	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely cause the client to crash, causing a denial of service.	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-050423/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22882		
Affected Version(s): * Up to (excluding) 5.13.3					
N/A	16-Mar-2023	7.5	Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. **CVE ID : CVE-2023-22880**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-050423/1207
Hardware					
Vendor: 360					
Product: d901					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	7.5	Stack Overflow vulnerability found in 360 D901 allows a remote attacker to cause a Distributed Denial of Service (DDOS) via a crafted HTTP package. **CVE ID : CVE-2023-27077**	N/A	H-360-D901-050423/1208
Vendor: centralite					
Product: pearl					
Affected Version(s): -					
N/A	17-Mar-2023	7.5	A vulnerability in Centralite Pearl Thermostat 0x04075010 allows attackers to cause a Denial of Service (DoS) via a crafted Zigbee message. **CVE ID : CVE-2023-24678**	N/A	H-CEN-PEAR-050423/1209
Vendor: Cisco					
Product: 8101-32fh					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8101-050423/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8101-050423/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8101-050423/1212
Product: 8101-32h					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-8101-050423/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8101-050423/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8101-050423/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8102-64h					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8102-050423/1216
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-8102-050423/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8102-050423/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8201					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8201-050423/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8201-050423/1220
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8201-050423/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8201-32fh					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8201-050423/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8201-050423/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8201-050423/1224
Product: 8202					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-8202-050423/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8202-050423/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8202-050423/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8800_12-slot					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8800-050423/1228
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-8800-050423/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8800-050423/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8800_18-slot					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8800-050423/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8800-050423/1232
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8800-050423/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8800_4-slot					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8800-050423/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8800-050423/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8800-050423/1236
Product: 8800_8-slot					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-8800-050423/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8800-050423/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8800-050423/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8804					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8804-050423/1240
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-8804-050423/1241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8804-050423/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8808					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8808-050423/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8808-050423/1244
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8808-050423/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8812					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8812-050423/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8812-050423/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8812-050423/1248
Product: 8818					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-8818-050423/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-8818-050423/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8818-050423/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 8831					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-8831-050423/1252
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-8831-050423/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-8831-050423/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: 9800-40					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-9800-050423/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-9800-050423/1256
Product: 9800-80					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-9800-050423/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-9800-050423/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: 9800-cl					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-9800-050423/1259
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-9800-050423/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Product: 9800-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-9800-050423/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-9800-050423/1262
Product: aironet_1540					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_1542d					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_1542i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1265
Product: aironet_1560					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_1562d					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_1562e					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1268
Product: aironet_1562i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_1800					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_1800i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1271
Product: aironet_1810					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_1810w					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_1815					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1274
Product: aironet_1815i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_1815m					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_1815t					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1277
Product: aironet_1815w					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_2800					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_2800e					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1280
Product: aironet_2800i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_3800					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_3800e					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1283
Product: aironet_3800i					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-AIRO-050423/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: aironet_3800p					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: aironet_4800					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-AIRO-050423/1286
Product: asr_1000					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1000-esp100					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1290
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ASR_-050423/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1000-esp100-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1294
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1000-esp200-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1298
Product: asr_1000-x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1299
Product: asr_1001					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1001-hx					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1303
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ASR_-050423/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1001-hx_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1307
Product: asr_1001-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ASR_-050423/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1311
Product: asr_1001-x_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1002					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1315
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ASR_-050423/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1002-hx					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ASR_-050423/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1319
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1002-hx_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1323
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: asr_1002-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_1002-x_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1328
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1004					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1331
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1006					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1335
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: asr_1006-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-	H-CIS-ASR_-050423/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1340
Product: asr_1009-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ASR_-050423/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_1013					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1345
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_1023					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1348
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_900					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1352
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: asr_9000					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_9000v					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1357
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): v2					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1360
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ASR_-050423/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_9001					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1364
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ASR_-050423/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	asaftdios-dhcpv6-cli-Zf3zTv	
Product: asr_9006					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1368
Product: asr_901-12c-f-d					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1369
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901-12c-ft-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1372
Product: asr_901-4c-f-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Product: asr_901-4c-ft-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1375
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901-6cz-f-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1378
Product: asr_901-6cz-f-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-ASR_-050423/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901-6cz-fs-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1381
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	y/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_901-6cz-fs-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1384
Product: asr_901-6cz-ft-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	https://sec.cloudapps.c	H-CIS-ASR_-050423/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901-6cz-ft-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1387
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_9010					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1391
Product: asr_901s-2sg-f-ah					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901s-2sg-f-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1394
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_901s-3sg-f-ah					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1397
Product: asr_901s-3sg-f-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1398
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_901s-4sg-f-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1401
Product: asr_902					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1404
Product: asr_902u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1405
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_903					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1408
Improper Limitation of a Pathname to a Restricted	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-ASR_-050423/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	rityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ASR_-050423/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: asr_907					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1412
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-ASR_-050423/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: asr_914					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Product: asr_920-10sz-pd					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1416
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-10sz-pd_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1419
Product: asr_920-12cz-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-ASR_-050423/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-12cz-a_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1422
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	y/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_920-12cz-d					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1425
Product: asr_920-12cz-d_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	https://sec.cloudapps.c	H-CIS-ASR_-050423/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-12sz-im					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1428
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_920-12sz-im_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_920-24sz-im					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1432
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-24sz-im_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1435
Product: asr_920-24sz-m					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ASR_-050423/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-24sz-m_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1438
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ASR_-050423/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Product: asr_920-24tz-m					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1441
Product: asr_920-24tz-m_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ASR_-050423/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-4sz-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1444
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ASR_-050423/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_920-4sz-a_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1447
Product: asr_920-4sz-d					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1448
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_920-4sz-d_r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1451
Product: asr_920u-12sz-im					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-ASR_-050423/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Product: asr_9901					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1454
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_9902					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1457
Product: asr_9903					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-ASR_-050423/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_9904					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1460
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ASR_-050423/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	y/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_9906					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1463
Product: asr_9910					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	https://sec.cloudapps.c	H-CIS-ASR_-050423/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: asr_9912					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1466
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ASR_-050423/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: asr_9920					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_9922					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ASR_-050423/1470
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ASR_-050423/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: catalyst_3650					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3650-12x48fd-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3650-12x48fd-l					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3650-12x48fd-s					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3650-12x48uq					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: catalyst_3650-12x48uq-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_3650-12x48uq-l					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1478
Product: catalyst_3650-12x48uq-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1479
Product: catalyst_3650-12x48ur					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1480
Product: catalyst_3650-12x48ur-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1481
Product: catalyst_3650-12x48ur-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1482
Product: catalyst_3650-12x48ur-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1483
Product: catalyst_3650-12x48uz					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1484
Product: catalyst_3650-12x48uz-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1485
Product: catalyst_3650-12x48uz-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1486
Product: catalyst_3650-12x48uz-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1487
Product: catalyst_3650-24pd					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1488
Product: catalyst_3650-24pd-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1489
Product: catalyst_3650-24pd-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1490
Product: catalyst_3650-24pd-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1491
Product: catalyst_3650-24pdm					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1492
Product: catalyst_3650-24pdm-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1493
Product: catalyst_3650-24pdm-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1494
Product: catalyst_3650-24pdm-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1495
Product: catalyst_3650-24ps-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1496
Product: catalyst_3650-24ps-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1497
Product: catalyst_3650-24ps-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1498
Product: catalyst_3650-24td-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1499
Product: catalyst_3650-24td-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1500
Product: catalyst_3650-24td-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1501
Product: catalyst_3650-24ts-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1502
Product: catalyst_3650-24ts-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1503
Product: catalyst_3650-24ts-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1504
Product: catalyst_3650-48fd-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1505
Product: catalyst_3650-48fd-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1506
Product: catalyst_3650-48fd-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1507
Product: catalyst_3650-48fq					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1508
Product: catalyst_3650-48fq-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1509
Product: catalyst_3650-48fq-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1510
Product: catalyst_3650-48fq-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1511
Product: catalyst_3650-48fqm					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1512
Product: catalyst_3650-48fqm-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1513
Product: catalyst_3650-48fqm-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1514
Product: catalyst_3650-48fqm-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1515
Product: catalyst_3650-48fs-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1516
Product: catalyst_3650-48fs-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1517
Product: catalyst_3650-48fs-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1518
Product: catalyst_3650-48pd-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1519
Product: catalyst_3650-48pd-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1520
Product: catalyst_3650-48pd-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1521
Product: catalyst_3650-48pq-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1522
Product: catalyst_3650-48pq-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1523
Product: catalyst_3650-48pq-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1524
Product: catalyst_3650-48ps-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1525
Product: catalyst_3650-48ps-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1526
Product: catalyst_3650-48ps-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1527
Product: catalyst_3650-48td-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1528
Product: catalyst_3650-48td-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1529
Product: catalyst_3650-48td-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1530
Product: catalyst_3650-48tq-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1531
Product: catalyst_3650-48tq-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1532
Product: catalyst_3650-48tq-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1533
Product: catalyst_3650-48ts-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1534
Product: catalyst_3650-48ts-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1535
Product: catalyst_3650-48ts-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1536
Product: catalyst_3650-8x24pd-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1537
Product: catalyst_3650-8x24pd-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1538
Product: catalyst_3650-8x24pd-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1539
Product: catalyst_3650-8x24uq					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1540
Product: catalyst_3650-8x24uq-e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1541
Product: catalyst_3650-8x24uq-l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1542
Product: catalyst_3650-8x24uq-s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1543
Product: catalyst_3850					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-12s-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1547
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-12s-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1551
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-12x48u					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1555
Product: catalyst_3850-12xs-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-12xs-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1559
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-16xs-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1563
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-16xs-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1567
Product: catalyst_3850-24p-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24p-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1571
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24p-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1575
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24pw-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1579
Product: catalyst_3850-24s-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24s-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1583
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24t-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1587
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24t-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1591
Product: catalyst_3850-24t-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24u					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1595
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24u-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1599
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24u-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1603
Product: catalyst_3850-24u-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xs					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1607
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xs-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1611
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xs-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1615
Product: catalyst_3850-24xu					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xu-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1619
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xu-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1623
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-24xu-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1627
Product: catalyst_3850-32xs-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-32xs-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1631
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48f-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1635
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48f-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1639
Product: catalyst_3850-48f-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48p-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1643
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48p-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1647
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48p-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1651
Product: catalyst_3850-48pw-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48t-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1655
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48t-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1659
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48t-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1663
Product: catalyst_3850-48u					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48u-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1667
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48u-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1671
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48u-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1675
Product: catalyst_3850-48xs					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48xs-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1679
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48xs-f-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1683
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-48xs-f-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1687
Product: catalyst_3850-48xs-s					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-nm-2-40g					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1691
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_3850-nm-8-10g					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1695
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8200					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1699
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CATA-050423/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: catalyst_8300					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-	H-CIS-CATA-050423/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_8300-1n1s-4t2x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1704
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8300-1n1s-6t					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1709
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8300-2n2s-4t2x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1713
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-CATA-050423/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8300-2n2s-6t					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1717
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8500					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1722
Product: catalyst_8500-4qc					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-CATA-050423/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1726
Product: catalyst_8500l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-CATA-050423/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_8510csr					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1731
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8510msr					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1736
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8540csr					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1740
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-CATA-050423/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_8540msr					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CATA-050423/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1744
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9100					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9105					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1748
Product: catalyst_9105ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9105axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9105axw					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1751
Product: catalyst_9115					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9115ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9115axe					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1754
Product: catalyst_9115axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9115_ap					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9117					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1757
Product: catalyst_9117ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9117axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9117_ap					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1760
Product: catalyst_9120					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9120ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9120axe					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1763
Product: catalyst_9120axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9120axp					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9120_ap					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1766
Product: catalyst_9124					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9124ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9124axd					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1769
Product: catalyst_9124axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9130					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9130ax					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1772
Product: catalyst_9130axe					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	
Product: catalyst_9130axi					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_9130_ap					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/1775
Product: catalyst_9200					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9200cx					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1779
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9200l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1783
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note:	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1788
Product: catalyst_9300-24p-a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1789
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-24p-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1793
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	ter/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE	https://sec.cloudapps.c	H-CIS-CATA-050423/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-24s-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1800
Product: catalyst_9300-24s-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-24t-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1805
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-CATA-050423/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-24t-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1811
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CATA-050423/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: catalyst_9300-24u-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-CATA-050423/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: catalyst_9300-24u-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1817
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-24ux-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1823
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-CATA-050423/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: catalyst_9300-24ux-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_9300-48p-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1829
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48p-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1833
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	https://sec.cloudapps.c	H-CIS-CATA-050423/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1835
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48s-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1840
Product: catalyst_9300-48s-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48t-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1845
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-CATA-050423/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48t-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1851
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CATA-050423/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: catalyst_9300-48u-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-CATA-050423/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: catalyst_9300-48u-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1857
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48un-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1863
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-CATA-050423/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: catalyst_9300-48un-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_9300-48uxm-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1869
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300-48uxm-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1873
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	https://sec.cloudapps.c	H-CIS-CATA-050423/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1875
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1880
Product: catalyst_9300l-24p-4g-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-24p-4g-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1885
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-CATA-050423/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-24p-4x-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1891
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CATA-050423/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: catalyst_9300l-24p-4x-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-CATA-050423/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: catalyst_9300l-24t-4g-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1897
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-24t-4g-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1903
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-CATA-050423/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: catalyst_9300l-24t-4x-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_9300l-24t-4x-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1909
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-48p-4g-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1913
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	https://sec.cloudapps.c	H-CIS-CATA-050423/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1915
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-48p-4g-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1920
Product: catalyst_9300l-48p-4x-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-48p-4x-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1925
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-CATA-050423/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-48t-4g-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1931
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CATA-050423/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: catalyst_9300l-48t-4g-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-	H-CIS-CATA-050423/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: catalyst_9300l-48t-4x-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1937
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300l-48t-4x-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1943
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-CATA-050423/1944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: catalyst_9300lm					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: catalyst_9300l_stack					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1949
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	H-CIS-CATA-050423/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9300x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1953
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	https://sec.cloudapps.c	H-CIS-CATA-050423/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1955
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9400					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1959
Product: catalyst_9400_supervisor_engine-1					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9407r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1963
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9410r					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1967
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9500					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1971
Product: catalyst_9500h					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9600					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1975
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9600x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1979
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9600_supervisor_engine-1					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1983
Product: catalyst_9800					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-40					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1987
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-40_wireless_controller					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1991
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-80					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1995
Product: catalyst_9800-80_wireless_controller					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-cl					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/1999
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-l					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2003
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800-l-c					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/2007
Product: catalyst_9800-l-f					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-CATA-050423/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_9800_embedded_wireless_controller					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2011
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CATA-050423/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: catalyst_ie3200					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2015
Product: catalyst_ie3200_rugged_switch					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-CATA-050423/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: catalyst_ie3300					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2018
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-CATA-050423/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Product: catalyst_ie3300_rugged_switch					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2021
Product: catalyst_ie3400					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	https://sec.cloudapps.cisco.com/security/cen	H-CIS-CATA-050423/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: catalyst_ie3400_heavy_duty_switch					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2024
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Product: catalyst_ie3400_rugged_switch					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2027
Product: catalyst_ie9300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CATA-050423/2028
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CATA-050423/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: catalyst_iw6300					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/2030
Product: catalyst_iw6300_ac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/2031
Product: catalyst_iw6300_dc					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Product: catalyst_iw6300_dcw					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-CATA-050423/2033
Product: cbr-8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CBR--050423/2034
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CBR--050423/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Product: cbr8_converged_broadband_router					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CBR8-050423/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: cg418-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CG41-050423/2037
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-CG41-050423/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-CG41-050423/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: cg522-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-CG52-050423/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-CG52-050423/2041
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-CG52-050423/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: cloud_services_router_1000v					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-CLOU-050423/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: csr_1000v					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-CSR_-050423/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
Product: esr-6300-con-k9					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESR--050423/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: esr-6300-ncp-k9					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESR--050423/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: esr6300					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESR6-050423/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESR6-050423/2048
Product: ess-3300-24t-con-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ESS--050423/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-24t-con-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2052
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ESS--050423/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-24t-ncp-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2056
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-24t-ncp-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2060
Product: ess-3300-con-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ESS--050423/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-con-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2064
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ESS--050423/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-ncp-a					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2068
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ess-3300-ncp-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ESS--050423/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS--050423/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS--050423/2072
Product: ess9300-10x-e					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ESS9-050423/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ESS9-050423/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ESS9-050423/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: esw6300					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	H-CIS-ESW6-050423/2076
Product: ie-3200-8p2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	H-CIS-IE-3-050423/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	rityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: ie-3200-8t2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-IE-3-050423/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: ie-3300-8p2s-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8p2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8t2s-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8t2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8t2x-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8t2x-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8u2x-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3300-8u2x-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3400-8p2s-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ie-3400-8p2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20081		
Product: ie-3400-8t2s-a					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ie-3400-8t2s-e					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-3-050423/2090
Product: ie-9310-26s2c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-9-050423/2091
Product: ie-9320-26s2c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-IE-9-050423/2092
Product: integrated_services_virtual_router					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-INTE-050423/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-INTE-050423/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-INTE-050423/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1000					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2096
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ISR_-050423/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Product: isr_1100					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2100
Product: isr_1100-4g					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ISR_-050423/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: isr_1100-4g\/6g					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2104
Product: isr_1100-4p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2105
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ISR_-050423/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1100-6g					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2109
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ISR_-050423/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1100-8p					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2113
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ISR_-050423/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1101					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2118
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1101-4p					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2122
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ISR_-050423/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	asaftdios-dhcpv6-cli-Zf3zTv	
Product: isr_1109					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-	H-CIS-ISR_-050423/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2127
Product: isr_1109-2p					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ISR_-050423/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ISR_-050423/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: isr_1109-4p					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2132
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ISR_-050423/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1111x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2136
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ISR_-050423/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1111x-8p					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2140
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_111x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2144
Product: isr_1120					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an	https://sec.cloudapps.cisco.com/s	H-CIS-ISR_-050423/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	H-CIS-ISR_-050423/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: isr_1131					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2149
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of	https://sec.cloudapps.cisco.com/s	H-CIS-ISR_-050423/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	ecurity/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_1160					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2154
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4000					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2157
Improper Limitation	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE	https://sec.cloudapps.c	H-CIS-ISR_-050423/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4221					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2162
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-	H-CIS-ISR_-050423/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	dhcpv6-cli-Zf3zTv	
Product: isr_4321					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2166
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security	https://sec.cloudapps.cisco.com/security/cen	H-CIS-ISR_-050423/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	ter/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
Product: isr_4331					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	H-CIS-ISR_-050423/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	y/cisco-sa-ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20066		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2171
Product: isr_4351					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2172
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ISR_-050423/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4431					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20035		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2177
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4451					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2181
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-	H-CIS-ISR_-050423/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4451-x					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2185
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-ISR_-050423/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: isr_4461					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	H-CIS-ISR_-050423/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	H-CIS-ISR_-050423/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	H-CIS-ISR_-050423/2190
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	H-CIS-ISR_-050423/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Vendor: dek-1705_project					
Product: dek-1705					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Mar-2023	9.8	DEK-1705 <=Firmware:34.23.1 device was discovered to have a command execution vulnerability. **CVE ID : CVE-2023-23149**	N/A	H-DEK-DEK--050423/2192
Vendor: Dell					
Product: embedded_box_pc_3000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Mar-2023	6.7	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with administrator privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-24571**	https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046	H-DEL-EMBE-050423/2193
Vendor: Dlink					
Product: dir820la1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp. **CVE ID : CVE-2023-25280**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR8-050423/2194
Out-of-bounds Write	16-Mar-2023	7.5	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the nextPage parameter to ping.ccp. **CVE ID : CVE-2023-25281**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR8-050423/2195
Vendor: hgiga					
Product: powerstation					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	8.8	HGiga PowerStation remote management function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service. **CVE ID : CVE-2023-24837**	https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html	H-HGI-POWE-050423/2196
Missing Authentication for Critical Function	27-Mar-2023	7.5	HGiga PowerStation has a vulnerability of Information Leakage. An unauthenticated remote attacker can exploit this vulnerability to obtain the administrator's credential, resulting in performing arbitrary system operation or disrupt service. **CVE ID : CVE-2023-24838**	https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html	H-HGI-POWE-050423/2197
Vendor: hpe					
Product: apollo_4200_gen10_plus_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: apollo_4200_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2199
Product: apollo_4200_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2200
Product: apollo_4510_gen10_system					
Affected Version(s): -					
Improper Neutralizat	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability	https://support.hpe.co	H-HPE-APOL-050423/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	m/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	
Product: apollo_6500_gen10_plus_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2202
Product: apollo_6500_gen10_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: apollo_n2600_gen10_plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2204
Product: apollo_n2800_gen10_plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2205
Product: apollo_r2000_chassis					
Affected Version(s): -					
Improper Neutralizat	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability	https://support.hpe.co	H-HPE-APOL-050423/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	m/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	
Product: apollo_r2200_gen10					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2207
Product: apollo_r2600_gen10					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: apollo_r2800_gen10					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-APOL-050423/2209
Product: aruba_cx_10000-48y6					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2210
Product: aruba_cx_6200f_48g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2211
Product: aruba_cx_6200m_24g					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2212
Product: aruba_cx_6300m_24p					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine.	https://www.arubanetworks.com/assets/alert/ARUBA-	H-HPE-ARUB-050423/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	PSA-2023-004.txt	
Product: aruba_cx_6300m_48g					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2214
Product: aruba_cx_6405					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**		
Product: aruba_cx_6410					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2216
Product: aruba_cx_8320-32					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1168		
Product: aruba_cx_8320-48p					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2218
Product: aruba_cx_8325-32c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2219
Product: aruba_cx_8325-48y8c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2220
Product: aruba_cx_8360-12c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2221
Product: aruba_cx_8360-16y2c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine.	https://www.arubanetworks.com/assets/alert/ARUBA-	H-HPE-ARUB-050423/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	PSA-2023-004.txt	
Product: aruba_cx_8360-24xf2c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2223
Product: aruba_cx_8360-32y4c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**		
Product: aruba_cx_8360-48xt4c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2225
Product: aruba_cx_8360-48y6c					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1168		
Product: aruba_cx_8400					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2227
Product: aruba_cx_9300_32d					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	H-HPE-ARUB-050423/2228
Product: edgeline_e920d_server_blade					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-EDGE-050423/2229
Product: edgeline_e920t_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-EDGE-050423/2230
Product: edgeline_e920_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-EDGE-050423/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_bl420c_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2232
Product: proliant_bl460c_gen10_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2233
Product: proliant_bl460c_gen8_server_blade					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2234
Product: proliant_bl460c_gen9_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2235
Product: proliant_bl465c_gen8_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_bl660c_gen8_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2237
Product: proliant_bl660c_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2238
Product: proliant_dl120_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2239
Product: proliant_dl120_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2240
Product: proliant_dl160_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl160_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2242
Product: proliant_dl160_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2243
Product: proliant_dl180_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2244
Product: proliant_dl180_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2245
Product: proliant_dl20_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl20_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2247
Product: proliant_dl20_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2248
Product: proliant_dl320e_gen8_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2249
Product: proliant_dl320e_gen8_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2250
Product: proliant_dl320_gen11_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl325_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2252
Product: proliant_dl325_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2253
Product: proliant_dl325_gen11_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2254
Product: proliant_dl345_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2255
Product: proliant_dl345_gen11_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl360e_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2257
Product: proliant_dl360p_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2258
Product: proliant_dl360_gen10_plus_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2259
Product: proliant_dl360_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2260
Product: proliant_dl360_gen11_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl360_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2262
Product: proliant_dl365_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2263
Product: proliant_dl365_gen11_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2264
Product: proliant_dl380e_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2265
Product: proliant_dl380p_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl380_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2267
Product: proliant_dl380_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2268
Product: proliant_dl380_gen11_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2269
Product: proliant_dl380_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2270
Product: proliant_dl385p_gen8_\(amd\)					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl385_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2272
Product: proliant_dl385_gen10_plus_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2273
Product: proliant_dl385_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2274
Product: proliant_dl385_gen11_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2275
Product: proliant_dl560_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl560_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2277
Product: proliant_dl560_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2278
Product: proliant_dl580_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2279
Product: proliant_dl580_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2280
Product: proliant_dl580_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dl60_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2282
Product: proliant_dl80_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2283
Product: proliant_dx170r_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2284
Product: proliant_dx190r_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2285
Product: proliant_dx220n_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dx325_gen10_plus_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2287
Product: proliant_dx360_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2288
Product: proliant_dx360_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2289
Product: proliant_dx380_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2290
Product: proliant_dx380_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_dx385_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2292
Product: proliant_dx385_gen10_plus_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2293
Product: proliant_dx4200_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2294
Product: proliant_dx560_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2295
Product: proliant_e910t_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_e910_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2297
Product: proliant_microserver_gen8					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2298
Product: proliant_ml110_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2299
Product: proliant_ml110_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2300
Product: proliant_ml30_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_ml30_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2302
Product: proliant_ml310e_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2303
Product: proliant_ml310e_gen8_v2_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2304
Product: proliant_ml350e_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2305
Product: proliant_ml350e_gen8_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_ml350p_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2307
Product: proliant_ml350_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2308
Product: proliant_ml350_gen11_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2309
Product: proliant_ml350_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2310
Product: proliant_sl210t_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_sl230s_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2312
Product: proliant_sl250s_gen8_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2313
Product: proliant_sl270s_gen8_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2314
Product: proliant_sl270s_gen8_se_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2315
Product: proliant_ws460c_gen8_graphics_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_ws460c_gen9_graphics_server_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2317
Product: proliant_xl170r_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2318
Product: proliant_xl170r_gen9_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2319
Product: proliant_xl190r_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2320
Product: proliant_xl190r_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_xl220a_gen8_v2_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2322
Product: proliant_xl220n_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2323
Product: proliant_xl225n_gen10_plus_1u_node					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2324
Product: proliant_xl230a_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2325
Product: proliant_xl230b_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_xl230k_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2327
Product: proliant_xl250a_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2328
Product: proliant_xl270d_gen10_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2329
Product: proliant_xl270d_gen9_special_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2330
Product: proliant_xl290n_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_xl450_gen10_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2332
Product: proliant_xl450_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2333
Product: proliant_xl645d_gen10_plus_server					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2334
Product: proliant_xl675d_gen10_plus_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2335
Product: proliant_xl730f_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: proliant_xl740f_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2337
Product: proliant_xl750f_gen9_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-PROL-050423/2338
Product: storage_file_controller					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2339
Product: storage_performance_file_controller					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2340
Product: storeeasy_1430_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_1440_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2342
Product: storeeasy_1450_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2343
Product: storeeasy_1460_storage					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2344
Product: storeeasy_1530_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2345
Product: storeeasy_1540_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_1550_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2347
Product: storeeasy_1560_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2348
Product: storeeasy_1630_storage					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2349
Product: storeeasy_1640_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2350
Product: storeeasy_1650_expanded_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_1650_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2352
Product: storeeasy_1660_expanded_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2353
Product: storeeasy_1660_performance_storage					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2354
Product: storeeasy_1660_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2355
Product: storeeasy_1830_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_1840_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2357
Product: storeeasy_1850_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2358
Product: storeeasy_1860_performance_storage					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2359
Product: storeeasy_1860_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2360
Product: storeeasy_3830_gateway_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_3830_gateway_storage_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2362
Product: storeeasy_3840_gateway_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2363
Product: storeeasy_3840_gateway_storage_blade					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2364
Product: storeeasy_3850_gateway_single_node_upgrade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2365
Product: storeeasy_3850_gateway_storage					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: storeeasy_3850_gateway_storage_blade					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2367
Product: storevirtual_3000_file_controller					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-STOR-050423/2368
Product: synergy_480_gen10_compute_module					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2369
Product: synergy_480_gen10_plus_compute_module					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2370
Product: synergy_480_gen9_compute_module					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**		
Product: synergy_620_gen9_compute_module					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2372
Product: synergy_660_gen10_compute_module					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2373
Product: synergy_660_gen9_compute_module					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2374
Product: synergy_680_gen9_compute_module					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	H-HPE-SYNE-050423/2375
Vendor: jcgcn.com					
Product: jhr-n916r					
Affected Version(s): -					
N/A	16-Mar-2023	9.8	Command execution vulnerability was discovered in JHR-N916R router firmware version<=21.11.1.1483. **CVE ID : CVE-2023-24795**	N/A	H-JCG-JHR--050423/2376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: lancombg					
Product: sa-wr915nd					
Affected Version(s): -					
N/A	16-Mar-2023	9.8	SA-WR915ND router firmware v17.35.1 was discovered to be vulnerable to code execution. **CVE ID : CVE-2023-23150**	N/A	H-LAN-SA-W-050423/2377
Vendor: Omron					
Product: sysmac_cj2h-cpu64					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2378
Product: sysmac_cj2h-cpu64-eip					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where	https://www.ia.omron.com/product/vulnera	H-OMR-SYSM-050423/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	bility/OMSR-2023-001_en.pdf	
Product: sysmac_cj2h-cpu65					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2380
Product: sysmac_cj2h-cpu65-eip					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2381
Product: sysmac_cj2h-cpu66					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu66-eip					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2383
Product: sysmac_cj2h-cpu67					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu67-eip					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2385
Product: sysmac_cj2h-cpu68					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu68-eip					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2387
Product: sysmac_cj2m-cpu11					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cj2m-cpu12					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2389
Product: sysmac_cj2m-cpu13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2390
Product: sysmac_cj2m-cpu14					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu15					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2392
Product: sysmac_cj2m-cpu31					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu32					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2394
Product: sysmac_cj2m-cpu33					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu34					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2396
Product: sysmac_cj2m-cpu35					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1e-e10dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2398
Product: sysmac_cp1e-e10dr-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2399
Product: sysmac_cp1e-e10dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e10dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2401
Product: sysmac_cp1e-e10dt1-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e10dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2403
Product: sysmac_cp1e-e14dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e14sdr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2405
Product: sysmac_cp1e-e20dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1e-e20sdr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2407
Product: sysmac_cp1e-e30dr-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2408
Product: sysmac_cp1e-e30sdr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2410
Product: sysmac_cp1e-e40sdr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e60sdr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2412
Product: sysmac_cp1e-na20dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-na20dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2414
Product: sysmac_cp1e-na20dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1h-x40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2416
Product: sysmac_cp1h-x40dt-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2417
Product: sysmac_cp1h-x40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1h-xa40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2419
Product: sysmac_cp1h-xa40dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1h-xa40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2421
Product: sysmac_cp1h-y20dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-el20dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2423
Product: sysmac_cp1l-em30dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-em30dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2425
Product: sysmac_cp1l-em30dt1-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2426
Product: sysmac_cp1l-em40dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-em40dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2428
Product: sysmac_cp1l-em40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l10dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2430
Product: sysmac_cp1l-l10dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l10dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2432
Product: sysmac_cp1l-l10dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-l10dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2434
Product: sysmac_cp1l-l14dr-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2435
Product: sysmac_cp1l-l14dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l14dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2437
Product: sysmac_cp1l-l14dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l14dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2439
Product: sysmac_cp1l-l20dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l20dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2441
Product: sysmac_cp1l-l20dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-l20dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2443
Product: sysmac_cp1l-l20dt1-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2444
Product: sysmac_cp1l-m30dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m30dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2446
Product: sysmac_cp1l-m30dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m30dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2448
Product: sysmac_cp1l-m30dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2450
Product: sysmac_cp1l-m40dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-m40dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2452
Product: sysmac_cp1l-m40dt-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2453
Product: sysmac_cp1l-m40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m60dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2455
Product: sysmac_cp1l-m60dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m60dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2457
Product: sysmac_cp1l-m60dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m60dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2459
Product: sysmac_cp2e-e14dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-e20dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2461
Product: sysmac_cp2e-e30dr-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2462
Product: sysmac_cp2e-e40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-e60dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2464
Product: sysmac_cp2e-n14dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n14dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2466
Product: sysmac_cp2e-n14dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n14dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2468
Product: sysmac_cp2e-n14dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n20dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2470
Product: sysmac_cp2e-n20dr-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2471
Product: sysmac_cp2e-n20dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n20dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2473
Product: sysmac_cp2e-n20dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n30dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2475
Product: sysmac_cp2e-n30dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n30dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2477
Product: sysmac_cp2e-n30dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n30dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2479
Product: sysmac_cp2e-n40dr-a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2480
Product: sysmac_cp2e-n40dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n40dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2482
Product: sysmac_cp2e-n40dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2484
Product: sysmac_cp2e-n60dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n60dr-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2486
Product: sysmac_cp2e-n60dt-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n60dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2488
Product: sysmac_cp2e-n60dt1-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2489
Product: sysmac_cp2e-s30dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s30dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2491
Product: sysmac_cp2e-s30dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s40dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2493
Product: sysmac_cp2e-s40dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s40dt1-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2495
Product: sysmac_cp2e-s60dr-a					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-s60dt-d					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2497
Product: sysmac_cp2e-s60dt1-d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2498
Product: sysmac_cs1w-drm21-v1					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cs1w-eip21					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2500
Product: sysmac_cs1w-etn21					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cs1w-fln22					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2502
Product: sysmac_cs1w-nc\[\]71					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cs1w-spu01-v2					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	H-OMR-SYSM-050423/2504
Product: sysmac_cs1w-spu02-v2					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	H-OMR-SYSM-050423/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Vendor: paradox					
Product: ipr512					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	7.5	An issue found in Paradox Security Systems IPR512 allows attackers to cause a denial of service via the login.html and login.xml parameters. **CVE ID : CVE-2023-24709**	N/A	H-PAR-IPR5-050423/2506
Vendor: Samsung					
Product: exynos					
Affected Version(s): -					
N/A	16-Mar-2023	9.1	Improper authorization implementation in Exynos baseband prior to SMR Mar-2023 Release 1 allows incorrect handling of unencrypted message.	https://security.samsungmobile.com/securityUpdate.smsb?year=20	H-SAM-EXYN-050423/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21455	23&month=03	
Product: exynos_1080					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2508
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2509
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos	https://semiconductor.samsung.com/support/quality-support/pr	H-SAM-EXYN-050423/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	oduct-security-updates/	
Product: exynos_2100					
Affected Version(s): -					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. **CVE ID : CVE-2023-21459**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	H-SAM-EXYN-050423/2511
Product: exynos_980					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2513
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2514
Product: exynos_auto_t5123					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory	https://semiconductor.samsung.com/support/quality-support/product-	H-SAM-EXYN-050423/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	security-updates/	
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2516
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2517
Product: exynos_modem_5123					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2518
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2519
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**		
Product: exynos_modem_5300					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2521
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26497		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-050423/2523
Vendor: sauter-controls					
Product: ey-as525f001					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	27-Mar-2023	6.5	An authenticated malicious user could acquire the simple mail transfer protocol (SMTP) Password in cleartext format, despite it being protected and hidden behind asterisks. The attacker could then perform further attacks using the SMTP credentials. **CVE ID : CVE-2023-27927**	N/A	H-SAU-EY-A-050423/2524
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	An authenticated malicious user could successfully upload a malicious image could	N/A	H-SAU-EY-A-050423/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a denial-of-service condition. **CVE ID : CVE-2023-28652**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could force all authenticated users, such as administrative users, to perform unauthorized actions by viewing the logs. This action would also grant the attacker privilege escalation. **CVE ID : CVE-2023-22300**	N/A	H-SAU-EY-A-050423/2526
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could provide a malicious link and trick an unsuspecting user into clicking on it. If clicked, the attacker could execute the malicious JavaScript (JS) payload in the target's security context. **CVE ID : CVE-2023-28650**	N/A	H-SAU-EY-A-050423/2527
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	A malicious user could leverage this vulnerability to escalate privileges or perform unauthorized actions in the context of the targeted privileged users. **CVE ID : CVE-2023-28655**	N/A	H-SAU-EY-A-050423/2528
Vendor: silabs					
Product: wireless_smart_ubiquitous_network_linux_border_router					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network. **CVE ID : CVE-2023-1262**	N/A	H-SIL-WIRE-050423/2529
Vendor: Tenda					
Product: ax3					
Affected Version(s): -					
Out-of-bounds Write	24-Mar-2023	8.8	Tenda AX3 V16.03.12.11 is vulnerable to Buffer Overflow via /goform/SetFirewallCfg. **CVE ID : CVE-2023-27042**	N/A	H-TEN-AX3-050423/2530
Product: g103					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	7.5	Command Injection vulnerability found in Tenda G103 v.1.0.05 allows an attacker to obtain sensitive information via a crafted package **CVE ID : CVE-2023-27079**	N/A	H-TEN-G103-050423/2531
Product: w20e					
Affected Version(s): -					
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6 (US_W20EV4.0br_v15.11.0.6(1068_1546_841)_CN_TDC) is vulnerable to Buffer Overflow via function formIPMacBindModify.	N/A	H-TEN-W20E-050423/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26805		
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6(US_W20EV4.0br_v15.11.0.6(1068_1546_841 is vulnerable to Buffer Overflow via function formSetSysTime, **CVE ID : CVE-2023-26806**	N/A	H-TEN-W20E-050423/2533
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the enabled parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-27135**	N/A	H-TOT-A710-050423/2534
Vendor: Tp-link					
Product: tl-mr3020					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a crafted request to the tftp endpoint. **CVE ID : CVE-2023-27078**	N/A	H-TP--TL-M-050423/2535
Vendor: ui					
Product: edgerouter_x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. This issue affects some unknown processing of the component NAT Configuration Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier VDB-223301 was assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. **CVE ID : CVE-2023-1456**	N/A	H-UI-EDGE-050423/2536
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	** DISPUTED ** A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. Affected is an unknown function of the component Static Routing Configuration Handler. The manipulation of the argument next-hop-interface leads to command injection. It is possible to launch the attack remotely. The exploit has been	N/A	H-UI-EDGE-050423/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-223302 is the identifier assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. **CVE ID : CVE-2023-1457**		
Operating System					
Vendor: 360					
Product: d901_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	7.5	Stack Overflow vulnerability found in 360 D901 allows a remote attacker to cause a Distributed Denial of Service (DDOS) via a crafted HTTP package. **CVE ID : CVE-2023-27077**	N/A	O-360-D901-050423/2538
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	O-APP-MACO-050423/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-25859**		
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25903**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2540
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26334**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2541
Out-of-bounds Read	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26335**		
Use After Free	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26336**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2543
Out-of-bounds Write	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26337**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26338**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2545
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26339**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2546
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-APP-MACO-050423/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26340**		
Vendor: centralite					
Product: pearl_firmware					
Affected Version(s): 0x04075010					
N/A	17-Mar-2023	7.5	A vulnerability in Centralite Pearl Thermostat 0x04075010 allows attackers to cause a Denial of Service (DoS) via a crafted Zigbee message. **CVE ID : CVE-2023-24678**	N/A	O-CEN-PEAR-050423/2548
Vendor: Cisco					
Product: ios					
Affected Version(s): 12.2\\(6\\)i1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2550
Affected Version(s): 15.1\\(2\\)sg1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-	O-CIS-IOS-050423/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sg2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2552
Affected Version(s): 15.1\\(2\\)sg3					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	https://sec.cloudapps.c	O-CIS-IOS-050423/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sg4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sg5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2555
Affected Version(s): 15.1\\(2\\)sg6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sg7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2557
Affected Version(s): 15.1\\(2\\)sg8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	https://sec.cloudapps.cisco.com/security/cen	O-CIS-IOS-050423/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(2\\)sy10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2560
Affected Version(s): 15.1\\(2\\)sy11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sy12					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2562
Affected Version(s): 15.1\\(2\\)sy13					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy14					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(2\\)sy15					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2565
Affected Version(s): 15.1\\(2\\)sy16					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sy16a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2567
Affected Version(s): 15.1\\(2\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(2\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2570
Affected Version(s): 15.1\\(2\\)sy4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(2\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2572
Affected Version(s): 15.1\\(2\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(2\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2575
Affected Version(s): 15.1\\(2\\)sy9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(3\\)svr10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2577
Affected Version(s): 15.1\\(3\\)svs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svt1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(3\\)svt3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2580
Affected Version(s): 15.1\\(3\\)svt4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(3\\)svu1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2582
Affected Version(s): 15.1\\(3\\)svu10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svu11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(3\\)svu2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2585
Affected Version(s): 15.1\\(3\\)svu20					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(3\\)svu21					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2587
Affected Version(s): 15.1\\(3\\)svv1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svv2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(3\\)svv3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2590
Affected Version(s): 15.1\\(3\\)svw					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(3\\)svw1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2592
Affected Version(s): 15.1\\(3\\)svx					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svx1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.1\\(4\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2595
Affected Version(s): 15.1\\(4\\)m12a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.1\\(4\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2597
Affected Version(s): 15.1\\(4\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(4\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(1\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2600
Affected Version(s): 15.2\\(1\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(1\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2602
Affected Version(s): 15.2\\(1\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(1\\)ey					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2605
Affected Version(s): 15.2\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2607
Affected Version(s): 15.2\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(1\\)sy0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2610
Affected Version(s): 15.2\\(1\\)sy1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2612
Affected Version(s): 15.2\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(1\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2615
Affected Version(s): 15.2\\(1\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(1\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2617
Affected Version(s): 15.2\\(1\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2620
Affected Version(s): 15.2\\(2\\)e10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)e10a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2622
Affected Version(s): 15.2\\(2\\)e10b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2625
Affected Version(s): 15.2\\(2\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2627
Affected Version(s): 15.2\\(2\\)e5a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e5b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2630
Affected Version(s): 15.2\\(2\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)e7b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2632
Affected Version(s): 15.2\\(2\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)e9a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2635
Affected Version(s): 15.2\\(2\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)ea1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2637
Affected Version(s): 15.2\\(2\\)ea2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)ea3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)eb					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2640
Affected Version(s): 15.2\\(2\\)eb1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)eb2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2642
Affected Version(s): 15.2\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)s0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)s0c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2645
Affected Version(s): 15.2\\(2\\)s0d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2647
Affected Version(s): 15.2\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)sc1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)sc3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2650
Affected Version(s): 15.2\\(2\\)sc4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2652
Affected Version(s): 15.2\\(2\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(2\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2655
Affected Version(s): 15.2\\(234k\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(2a\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2657
Affected Version(s): 15.2\\(2a\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2b\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(3\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2660
Affected Version(s): 15.2\\(3\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(3\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2662
Affected Version(s): 15.2\\(3\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(3\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(3\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2665
Affected Version(s): 15.2\\(3\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(3a\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2667
Affected Version(s): 15.2\\(3m\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(3m\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(3m\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2670
Affected Version(s): 15.2\\(4\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2672
Affected Version(s): 15.2\\(4\\)e10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)e10a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)e10b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2675
Affected Version(s): 15.2\\(4\\)e10c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2677
Affected Version(s): 15.2\\(4\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2680
Affected Version(s): 15.2\\(4\\)e5a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2682
Affected Version(s): 15.2\\(4\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)e9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2685
Affected Version(s): 15.2\\(4\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)ea1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2687
Affected Version(s): 15.2\\(4\\)ea2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)ea3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)ea4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2690
Affected Version(s): 15.2\\(4\\)ea5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)ea6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2692
Affected Version(s): 15.2\\(4\\)ea7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)ea8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)ea9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2695
Affected Version(s): 15.2\\(4\\)ea9a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)ec1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2697
Affected Version(s): 15.2\\(4\\)ec2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)gc1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)gc2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2700
Affected Version(s): 15.2\\(4\\)gc3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2702
Affected Version(s): 15.2\\(4\\)m11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2705
Affected Version(s): 15.2\\(4\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)m6b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2707
Affected Version(s): 15.2\\(4\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2710
Affected Version(s): 15.2\\(4\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)s0c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2712
Affected Version(s): 15.2\\(4\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)s1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2715
Affected Version(s): 15.2\\(4\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)s3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2717
Affected Version(s): 15.2\\(4\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)s4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2720
Affected Version(s): 15.2\\(4\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2722
Affected Version(s): 15.2\\(4\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4m\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4m\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2725
Affected Version(s): 15.2\\(4m\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4n\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2727
Affected Version(s): 15.2\\(4o\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4o\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(4p\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2730
Affected Version(s): 15.2\\(4q\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(4s\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2732
Affected Version(s): 15.2\\(5\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(5\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(5\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2735
Affected Version(s): 15.2\\(5\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(5\\)e2c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2737
Affected Version(s): 15.2\\(5\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(5\\)ex					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(5a\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2740
Affected Version(s): 15.2\\(5a\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(5b\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2742
Affected Version(s): 15.2\\(5c\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(6\\)e0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2745
Affected Version(s): 15.2\\(6\\)e0c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(6\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2747
Affected Version(s): 15.2\\(6\\)e1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)e1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(6\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2750
Affected Version(s): 15.2\\(6\\)e2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(6\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2752
Affected Version(s): 15.2\\(6\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)eb					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(7\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2755
Affected Version(s): 15.2\\(7\\)e0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(7\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2757
Affected Version(s): 15.2\\(7\\)e0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(7\\)e1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2760
Affected Version(s): 15.2\\(7\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(7\\)e2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2762
Affected Version(s): 15.2\\(7\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(7\\)e3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2765
Affected Version(s): 15.2\\(7\\)e3k					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(7\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2767
Affected Version(s): 15.2\\(7\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.2\\(7a\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2770
Affected Version(s): 15.2\\(7b\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.2\\(8\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2772
Affected Version(s): 15.2\\(8\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(8\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(0\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2775
Affected Version(s): 15.3\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2777
Affected Version(s): 15.3\\(1\\)s1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2780
Affected Version(s): 15.3\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2782
Affected Version(s): 15.3\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2785
Affected Version(s): 15.3\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2787
Affected Version(s): 15.3\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2790
Affected Version(s): 15.3\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2792
Affected Version(s): 15.3\\(3\\)s1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(3\\)s2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2795
Affected Version(s): 15.3\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2797
Affected Version(s): 15.3\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.3\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2800
Affected Version(s): 15.3\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.3\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2802
Affected Version(s): 15.3\\(3\\)s8a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(1\\)cg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2805
Affected Version(s): 15.4\\(1\\)cg1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2807
Affected Version(s): 15.4\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2810
Affected Version(s): 15.4\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2812
Affected Version(s): 15.4\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2815
Affected Version(s): 15.4\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2817
Affected Version(s): 15.4\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2820
Affected Version(s): 15.4\\(1\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(2\\)cg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2822
Affected Version(s): 15.4\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2825
Affected Version(s): 15.4\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2827
Affected Version(s): 15.4\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2830
Affected Version(s): 15.4\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2832
Affected Version(s): 15.4\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2835
Affected Version(s): 15.4\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2837
Affected Version(s): 15.4\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2840
Affected Version(s): 15.4\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2842
Affected Version(s): 15.4\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)m7a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2845
Affected Version(s): 15.4\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2847
Affected Version(s): 15.4\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s0d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)s0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2850
Affected Version(s): 15.4\\(3\\)s0f					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2852
Affected Version(s): 15.4\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2855
Affected Version(s): 15.4\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2857
Affected Version(s): 15.4\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.4\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2860
Affected Version(s): 15.4\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.4\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2862
Affected Version(s): 15.4\\(3\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)sn1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2865
Affected Version(s): 15.5\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2867
Affected Version(s): 15.5\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(1\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2870
Affected Version(s): 15.5\\(1\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2872
Affected Version(s): 15.5\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2875
Affected Version(s): 15.5\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(1\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2877
Affected Version(s): 15.5\\(1\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(1\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(1\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2880
Affected Version(s): 15.5\\(1\\)sy9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2882
Affected Version(s): 15.5\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2885
Affected Version(s): 15.5\\(1\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2887
Affected Version(s): 15.5\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2890
Affected Version(s): 15.5\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2892
Affected Version(s): 15.5\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2895
Affected Version(s): 15.5\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2897
Affected Version(s): 15.5\\(2\\)xb					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2900
Affected Version(s): 15.5\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2902
Affected Version(s): 15.5\\(3\\)m11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m11a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2905
Affected Version(s): 15.5\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2907
Affected Version(s): 15.5\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)m4b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2910
Affected Version(s): 15.5\\(3\\)m4c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2912
Affected Version(s): 15.5\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2915
Affected Version(s): 15.5\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2917
Affected Version(s): 15.5\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2920
Affected Version(s): 15.5\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)s10a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2922
Affected Version(s): 15.5\\(3\\)s10b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2925
Affected Version(s): 15.5\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2927
Affected Version(s): 15.5\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2930
Affected Version(s): 15.5\\(3\\)s6b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2932
Affected Version(s): 15.5\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.5\\(3\\)s9a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2935
Affected Version(s): 15.5\\(3\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.5\\(3\\)sn0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2937
Affected Version(s): 15.6\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2940
Affected Version(s): 15.6\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2942
Affected Version(s): 15.6\\(1\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(1\\)sn2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2945
Affected Version(s): 15.6\\(1\\)sn3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2947
Affected Version(s): 15.6\\(1\\)t0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2950
Affected Version(s): 15.6\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2952
Affected Version(s): 15.6\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2955
Affected Version(s): 15.6\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2957
Affected Version(s): 15.6\\(2\\)sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)sp1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(2\\)sp2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2960
Affected Version(s): 15.6\\(2\\)sp3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(2\\)sp4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2962
Affected Version(s): 15.6\\(2\\)sp5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)sp6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(2\\)sp7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2965
Affected Version(s): 15.6\\(2\\)sp8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(2\\)sp8a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2967
Affected Version(s): 15.6\\(2\\)sp9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(2\\)t0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2970
Affected Version(s): 15.6\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2972
Affected Version(s): 15.6\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2975
Affected Version(s): 15.6\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(3\\)m1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2977
Affected Version(s): 15.6\\(3\\)m1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2980
Affected Version(s): 15.6\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2982
Affected Version(s): 15.6\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2985
Affected Version(s): 15.6\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(3\\)m6b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2987
Affected Version(s): 15.6\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2990
Affected Version(s): 15.6\\(3\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.6\\(4\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2992
Affected Version(s): 15.6\\(5\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(7\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.6\\(7\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2995
Affected Version(s): 15.6\\(7\\)sn2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.7\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2997
Affected Version(s): 15.7\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.7\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/2999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.7\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3000
Affected Version(s): 15.7\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.7\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3002
Affected Version(s): 15.7\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.7\\(3\\)m4b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.7\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3005
Affected Version(s): 15.7\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.7\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3007
Affected Version(s): 15.7\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.7\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.8\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3010
Affected Version(s): 15.8\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.8\\(3\\)m0b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3012
Affected Version(s): 15.8\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.8\\(3\\)m1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.8\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3015
Affected Version(s): 15.8\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.8\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3017
Affected Version(s): 15.8\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.8\\(3\\)m3b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.8\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3020
Affected Version(s): 15.8\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.8\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3022
Affected Version(s): 15.8\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.8\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.9\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3025
Affected Version(s): 15.9\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.9\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3027
Affected Version(s): 15.9\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.9\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.9\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3030
Affected Version(s): 15.9\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 15.9\\(3\\)m3b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3032
Affected Version(s): 15.9\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS-050423/3033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.9\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 15.9\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS-050423/3035
Affected Version(s): 17.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	O-CIS-IOS-050423/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Product: ios_xe					
Affected Version(s): 17.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	O-CIS-IOS_-050423/3037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. **CVE ID : CVE-2023-20081**		
Affected Version(s): * Up to (excluding) 16.12.8					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	O-CIS-IOS_-050423/3038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Affected Version(s): * Up to (excluding) 17.3.7					
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	O-CIS-IOS_-050423/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Affected Version(s): 16.1.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3040
Affected Version(s): 16.1.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IOS_-050423/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.1.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3042
Affected Version(s): 16.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3043
Affected Version(s): 16.10.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.10.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3045
Affected Version(s): 16.10.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-	O-CIS-IOS_-050423/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	dos-44cMvdDK	
Affected Version(s): 16.10.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3047
Affected Version(s): 16.10.1e					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	https://sec.cloudapps.c	O-CIS-IOS_-050423/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.10.1f					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.10.1g					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3050
Affected Version(s): 16.10.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.10.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3052
Affected Version(s): 16.10.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	https://sec.cloudapps.cisco.com/security/cen	O-CIS-IOS_-050423/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.11.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.11.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3055
Affected Version(s): 16.11.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.11.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3057
Affected Version(s): 16.11.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.11.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.12.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3060
Affected Version(s): 16.12.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.12.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3062
Affected Version(s): 16.12.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.1t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.12.1w					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3065
Affected Version(s): 16.12.1x					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.12.1y					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3067
Affected Version(s): 16.12.1z					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.1z1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.12.1z2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3070
Affected Version(s): 16.12.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.12.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3072
Affected Version(s): 16.12.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.2t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.12.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3075
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	O-CIS-IOS_-050423/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Affected Version(s): 16.12.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3077
Affected Version(s): 16.12.3s					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	https://sec.cloudapps.c	O-CIS-IOS_-050423/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.12.4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3080
Affected Version(s): 16.12.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.12.5a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3082
Affected Version(s): 16.12.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	https://sec.cloudapps.cisco.com/security/cen	O-CIS-IOS_-050423/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.12.6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3085
Affected Version(s): 16.12.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.2.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3087
Affected Version(s): 16.2.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.3.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.3.10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3090
Affected Version(s): 16.3.11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.3.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3092
Affected Version(s): 16.3.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.3.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.3.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3095
Affected Version(s): 16.3.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.3.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3097
Affected Version(s): 16.3.6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.3.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.3.8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3100
Affected Version(s): 16.3.9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.4.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3102
Affected Version(s): 16.4.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.4.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.5.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3105
Affected Version(s): 16.5.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.5.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3107
Affected Version(s): 16.5.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.5.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.6.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3110
Affected Version(s): 16.6.10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.6.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3112
Affected Version(s): 16.6.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.6.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.6.4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3115
Affected Version(s): 16.6.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.6.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3117
Affected Version(s): 16.6.5a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.6.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.6.6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3120
Affected Version(s): 16.6.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.6.7a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3122
Affected Version(s): 16.6.8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.6.9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.7.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3125
Affected Version(s): 16.7.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.7.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3127
Affected Version(s): 16.7.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.7.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.7.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3130
Affected Version(s): 16.8.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.8.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3132
Affected Version(s): 16.8.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.8.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.8.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3135
Affected Version(s): 16.8.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.8.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3137
Affected Version(s): 16.8.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.8.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.9.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3140
Affected Version(s): 16.9.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.9.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3142
Affected Version(s): 16.9.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.9.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3145
Affected Version(s): 16.9.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.9.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3147
Affected Version(s): 16.9.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.9.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3150
Affected Version(s): 16.9.3h					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.9.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3152
Affected Version(s): 16.9.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.4c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.9.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3155
Affected Version(s): 16.9.5f					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 16.9.6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3157
Affected Version(s): 16.9.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 16.9.8a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3160
Affected Version(s): 16.9.8b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.1.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3162
Affected Version(s): 17.1.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.1.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 17.1.1t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3165
Affected Version(s): 17.1.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.1.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3167
Affected Version(s): 17.11.1					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. **CVE ID : CVE-2023-20065**	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Affected Version(s): 17.2.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 17.2.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3170
Affected Version(s): 17.2.1r					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.2.1v					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3172
Affected Version(s): 17.2.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.2.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 17.3.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3175
Affected Version(s): 17.3.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.3.1w					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3177
Affected Version(s): 17.3.1x					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.3.1z					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 17.3.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3180
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	O-CIS-IOS_-050423/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Affected Version(s): 17.3.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3182
Affected Version(s): 17.3.3					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	https://sec.cloudapps.c	O-CIS-IOS_-050423/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.3.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.4.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3185
Affected Version(s): 17.4.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 17.4.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3187
Affected Version(s): 17.4.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	https://sec.cloudapps.cisco.com/security/cen	O-CIS-IOS_-050423/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.4.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 17.4.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3190
Affected Version(s): 17.6.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	O-CIS-IOS_-050423/3191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. **CVE ID : CVE-2023-20066**		
Affected Version(s): 17.6.3					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	O-CIS-IOS_-050423/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20065		
Affected Version(s): 17.7					
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	O-CIS-IOS_-050423/3193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
Affected Version(s): 17.9.1					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. **CVE ID : CVE-2023-20072**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5	O-CIS-IOS_-050423/3194
Affected Version(s): 17.9.1a					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling	https://sec.cloudapps.c	O-CIS-IOS_-050423/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. **CVE ID : CVE-2023-20072**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5	
Affected Version(s): 17.9.1w					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5	O-CIS-IOS_-050423/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. **CVE ID : CVE-2023-20072**		
Affected Version(s): 3.10.0ce					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.10.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3198
Affected Version(s): 3.10.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.10.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3200
Affected Version(s): 3.10.1ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	https://sec.cloudapps.cisco.com/security/cen	O-CIS-IOS_-050423/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.10.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3203
Affected Version(s): 3.10.1se					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.10.1xbs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3205
Affected Version(s): 3.10.1xcs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.10.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3208
Affected Version(s): 3.10.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.10.2ts					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3210
Affected Version(s): 3.10.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.10.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3213
Affected Version(s): 3.10.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.10.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3215
Affected Version(s): 3.10.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.8as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.10.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3218
Affected Version(s): 3.10.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.11.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3220
Affected Version(s): 3.11.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.1ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.11.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3223
Affected Version(s): 3.11.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.11.2ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3225
Affected Version(s): 3.11.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.11.3ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3228
Affected Version(s): 3.11.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.11.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3230
Affected Version(s): 3.11.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.11.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3233
Affected Version(s): 3.11.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.12.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3235
Affected Version(s): 3.12.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.12.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.12.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3238
Affected Version(s): 3.12.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.12.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3240
Affected Version(s): 3.13.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.13.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3243
Affected Version(s): 3.13.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.13.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3245
Affected Version(s): 3.13.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.13.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3248
Affected Version(s): 3.13.5as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.13.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3250
Affected Version(s): 3.13.6as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.6bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.13.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3253
Affected Version(s): 3.13.7as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.13.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3255
Affected Version(s): 3.13.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.14.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3258
Affected Version(s): 3.14.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.14.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3260
Affected Version(s): 3.14.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.14.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.15.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3263
Affected Version(s): 3.15.1cs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.15.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3265
Affected Version(s): 3.15.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.15.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.15.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3268
Affected Version(s): 3.16.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.0bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3270
Affected Version(s): 3.16.0cs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.10as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3273
Affected Version(s): 3.16.10bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3275
Affected Version(s): 3.16.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3278
Affected Version(s): 3.16.2bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3280
Affected Version(s): 3.16.3as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.4as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3283
Affected Version(s): 3.16.4bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.4cs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3285
Affected Version(s): 3.16.4ds					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.4es					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.4gs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3288
Affected Version(s): 3.16.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.5as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3290
Affected Version(s): 3.16.5bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.6bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3293
Affected Version(s): 3.16.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.16.7as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3295
Affected Version(s): 3.16.7bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.16.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3298
Affected Version(s): 3.16.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.17.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3300
Affected Version(s): 3.17.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.17.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.17.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3303
Affected Version(s): 3.17.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.17.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3305
Affected Version(s): 3.18.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.18.0sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3308
Affected Version(s): 3.18.1asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.18.1bsp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3310
Affected Version(s): 3.18.1csp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.1gsp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.18.1hsp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3313
Affected Version(s): 3.18.1isp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.18.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3315
Affected Version(s): 3.18.1sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.2asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.18.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3318
Affected Version(s): 3.18.2sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.18.3asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3320
Affected Version(s): 3.18.3bsp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.18.3sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3323
Affected Version(s): 3.18.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.18.4sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3325
Affected Version(s): 3.18.5sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.6sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.18.7sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3328
Affected Version(s): 3.18.8asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.18.8sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3330
Affected Version(s): 3.18.9sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.3.0xo					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.3.1xo					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3333
Affected Version(s): 3.3.2xo					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.4.0sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3335
Affected Version(s): 3.4.1sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.4.2sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.4.3sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3338
Affected Version(s): 3.4.4sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.4.5sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3340
Affected Version(s): 3.4.6sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.4.7sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.4.8sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3343
Affected Version(s): 3.5.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.5.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3345
Affected Version(s): 3.5.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.5.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.6.0ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3348
Affected Version(s): 3.6.0be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.6.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3350
Affected Version(s): 3.6.10e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.6.2ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3353
Affected Version(s): 3.6.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.6.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3355
Affected Version(s): 3.6.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.5ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.6.5be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3358
Affected Version(s): 3.6.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.6.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3360
Affected Version(s): 3.6.7ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.7be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.6.7e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3363
Affected Version(s): 3.6.8e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.6.9ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3365
Affected Version(s): 3.6.9e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.0bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.7.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3368
Affected Version(s): 3.7.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.7.0xas					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3370
Affected Version(s): 3.7.0xbs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.7.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3373
Affected Version(s): 3.7.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.7.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3375
Affected Version(s): 3.7.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.2ts					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.7.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3378
Affected Version(s): 3.7.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.7.4as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3380
Affected Version(s): 3.7.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.7.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3383
Affected Version(s): 3.7.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.7.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3385
Affected Version(s): 3.7.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.8.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3388
Affected Version(s): 3.8.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.8.10ce					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3390
Affected Version(s): 3.8.10e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.8.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.8.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3393
Affected Version(s): 3.8.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.8.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3395
Affected Version(s): 3.8.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.8.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.8.5ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3398
Affected Version(s): 3.8.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.8.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3400
Affected Version(s): 3.8.7e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.8.8e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.8.9e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3403
Affected Version(s): 3.9.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.9.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3405
Affected Version(s): 3.9.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.9.0xas					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.9.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3408
Affected Version(s): 3.9.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**		
Affected Version(s): 3.9.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3410
Affected Version(s): 3.9.2be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu	O-CIS-IOS_-050423/3411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	rityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.9.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20080		
Affected Version(s): 3.9.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. **CVE ID : CVE-2023-20080**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3413
Affected Version(s): From (including) 17.1 Up to (excluding) 17.3.6					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	O-CIS-IOS_-050423/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**		
Affected Version(s): From (including) 17.4 Up to (excluding) 17.6.5					
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ	O-CIS-IOS_-050423/3415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. **CVE ID : CVE-2023-20082**		
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	O-CIS-IOS_-050423/3416
Affected Version(s): From (including) 17.7 Up to (excluding) 17.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. **CVE ID : CVE-2023-20056**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu	O-CIS-IOS_-050423/3417
Product: ios_xe_sd-wan					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	O-CIS-IOS_-050423/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. **CVE ID : CVE-2023-20035**		
Vendor: contiki-ng					
Product: contiki-ng					
Affected Version(s): * Up to (including) 4.8					
Out-of-bounds Write	17-Mar-2023	9.8	Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BLE L2CAP module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing of packets, with the size of PACKETBUF_SIZE. In	https://github.com/contiki-ng/contiki-ng/pull/2398, https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-m737-4vx6-pfqp	O-CON-CONT-050423/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger then the actual size of the packetbuf. When large packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. The problem can be worked around by applying the patch manually. **CVE ID : CVE-2023-28116**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	O-DEB-DEBI-050423/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.0					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	O-DEB-DEBI-050423/3421
Affected Version(s): 12.0					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	O-DEB-DEBI-050423/3422
Vendor: dek-1705_project					
Product: dek-1705_firmware					
Affected Version(s): 34.23.1					
Improper Neutralization of Special Elements used in a	24-Mar-2023	9.8	DEK-1705 <=Firmware:34.23.1 device was discovered to have a command execution vulnerability.	N/A	O-DEK-DEK--050423/3423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			**CVE ID : CVE-2023-23149**		
Vendor: Dell					
Product: embedded_box_pc_3000_firmware					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	16-Mar-2023	6.7	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with administrator privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-24571**	https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046	O-DEL-EMBE-050423/3424
Vendor: Dlink					
Product: dir820la1_firmware					
Affected Version(s): 105b03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp. **CVE ID : CVE-2023-25280**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR8-050423/3425
Out-of-bounds Write	16-Mar-2023	7.5	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR8-050423/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nextPage parameter to ping.ccp. **CVE ID : CVE-2023-25281**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). **CVE ID : CVE-2023-28333**	https://moodle.org/mod/forum/discuss.php?d=445065	O-FED-FEDO-050423/3427
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-FED-FEDO-050423/3428
Authorization Bypass Through User-	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store	https://dino.im/security/cve-2023-28686/	O-FED-FEDO-050423/3429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**		
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	O-FED-FEDO-050423/3430
Affected Version(s): 37					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-FED-FEDO-050423/3431
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**	https://dino.im/security/cve-2023-28686/	O-FED-FEDO-050423/3432
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4,	O-FED-FEDO-050423/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	
Allocation of Resources Without Limits or Throttling	23-Mar-2023	5.5	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to allocate and initialize a huge number of page tables to be used as a ring of descriptors for CQ and async events, potentially leading to an out-of-bounds read and crash of QEMU. **CVE ID : CVE-2023-1544**	https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html, https://bugzilla.redhat.com/show_bug.cgi?id=2180364	O-FED-FEDO-050423/3434
Affected Version(s): 38					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change	https://dino.im/security/cve-2023-28686/	O-FED-FEDO-050423/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. **CVE ID : CVE-2023-28686**		
Vendor: Google					
Product: android					
Affected Version(s): -					
Out-of-bounds Write	24-Mar-2023	9.8	In ProfSixDecomTcpSACKoption of RohcPacketCommon, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244450646References: N/A **CVE ID : CVE-2023-21057**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3436
Out-of-bounds Write	24-Mar-2023	9.8	In lcsm_SendRrAcquiAssist of lcsm_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-246169606References: N/A **CVE ID : CVE-2023-21058**		
N/A	24-Mar-2023	7.8	In buildCommand of bluetooth_ccc.cc, there is a possible out of bounds write 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 kernelAndroid ID: A-238420277References: N/A **CVE ID : CVE-2023-21040**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3438
Out-of-bounds Write	24-Mar-2023	7.8	In append_to_params of param_util.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-250123688References: N/A	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21041		
N/A	24-Mar-2023	7.8	In (TBD) of (TBD), there is a possible way to boot with a hidden debug policy due to a missing warning to the user. This could lead to local escalation of privilege after preparing the device, hiding the warning, and passing the phone to a new user, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243433344References: N/A **CVE ID : CVE-2023-21068**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3440
Out-of-bounds Read	24-Mar-2023	7.5	In sms_GetTpPiIe of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253770924References: N/A	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21060		
Out-of-bounds Read	24-Mar-2023	7.5	In EUTRAN_LCS_DecodeFacilityInformationElement of LPP_LcsManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-247564044References: N/A **CVE ID : CVE-2023-21059**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3442
Out-of-bounds Read	24-Mar-2023	7.5	In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-251805610References: N/A	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21053		
N/A	24-Mar-2023	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-254114726References: N/A **CVE ID : CVE-2023-21067**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3444
N/A	24-Mar-2023	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-229255400References: N/A **CVE ID : CVE-2023-21061**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3445
Out-of-bounds Write	24-Mar-2023	7.2	In EUTRAN_LCS_ConvertLCS_MOLRReq of LPP_CommonUtil.c, there is a possible out of bounds write due to a logic error in the code. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244556535References: N/A **CVE ID : CVE-2023-21054**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3446
Out-of-bounds Write	24-Mar-2023	6.7	In cs40l2x_cp_trigger_queue_show of cs40l2x.c, there is a possible out of	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-224000736References: N/A **CVE ID : CVE-2023-21038**	/pixel/2023-03-01	
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257289560References: N/A **CVE ID : CVE-2023-21077**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3448
Use After Free	24-Mar-2023	6.7	In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-239873326References: N/A **CVE ID : CVE-2023-21042**		
Use After Free	24-Mar-2023	6.7	In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239872581References: N/A **CVE ID : CVE-2023-21043**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3450
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254840211References: N/A **CVE ID : CVE-2023-21078**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	6.7	In load_png_image of ExynosHWCHelper.cpp, 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.Product: AndroidVersions: Android kernelAndroid ID: A-244423702References: N/A **CVE ID : CVE-2023-21050**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3452
Out-of-bounds Write	24-Mar-2023	6.7	In dwc3_exynos_clk_get of dwc3-exynos.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323322References: N/A **CVE ID : CVE-2023-21051**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3453
Out-of-bounds Write	24-Mar-2023	6.7	In setToExternal of ril_external_client.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3454

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.Product: AndroidVersions: Android kernelAndroid ID: A-259063189References: N/A **CVE ID : CVE-2023-21052**	/pixel/2023-03-01	
Access of Resource Using Incompatible Type ('Type Confusion')	24-Mar-2023	6.7	In lwis_slc_buffer_free of lwis_device_slc.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-245300559References: N/A **CVE ID : CVE-2023-21056**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3455
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: A-254839721References: N/A **CVE ID : CVE-2023-21079**		
Out-of-bounds Read	24-Mar-2023	6.7	In DoSetTempEcc of imsservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243376770References: N/A **CVE ID : CVE-2023-21062**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3457
Out-of-bounds Read	24-Mar-2023	6.7	In ParseWithAuthType of simdata.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243129862References: N/A **CVE ID : CVE-2023-21063**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Mar-2023	6.7	In DoSetPinControl of miscservice.cpp, there is a possible out of bounds read 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.Product: AndroidVersions: Android kernelAndroid ID: A-243130078References: N/A **CVE ID : CVE-2023-21064**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3459
Integer Overflow or Wraparound	24-Mar-2023	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 kernelAndroid ID: A-239630493References: N/A **CVE ID : CVE-2023-21065**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3460
Out-of-bounds Write	24-Mar-2023	6.7	In wl_update_hidden_ap_ie of wl_cfgscan.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254029309References: N/A **CVE ID : CVE-2023-21069**		
Out-of-bounds Write	24-Mar-2023	6.7	In add_roam_cache_list of wl_roam.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-254028776References: N/A **CVE ID : CVE-2023-21070**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3462
Out-of-bounds Write	24-Mar-2023	6.7	In dhd_prot_ioctcmplt_process of dhd_msgbuf.c, 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.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android kernelAndroid ID: A-254028518References: N/A **CVE ID : CVE-2023-21071**		
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A **CVE ID : CVE-2023-21072**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3464
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A **CVE ID : CVE-2023-21073**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	6.7	In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A **CVE ID : CVE-2023-21075**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3466
Out-of-bounds Write	24-Mar-2023	6.7	In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A **CVE ID : CVE-2023-21076**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3467
Use After Free	24-Mar-2023	6.4	In dit_hal_ioctl of dit.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244301523References: N/A **CVE ID : CVE-2023-21055**	/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	In BitmapExport.java, there is a possible failure to truncate images due to a logic error in the code.Product: AndroidVersions: Android kernelAndroid ID: A-264261868References: N/A **CVE ID : CVE-2023-21036**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3469
Out-of-bounds Read	24-Mar-2023	4.4	In dumpstateBoard of Dumpstate.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783650References: N/A **CVE ID : CVE-2023-21039**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Mar-2023	4.4	In init of VendorGraphicBufferMeta, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253425086References: N/A **CVE ID : CVE-2023-21044**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3471
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Mar-2023	4.4	In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-256166866References: N/A **CVE ID : CVE-2023-21047**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3472
Out-of-bounds Write	24-Mar-2023	4.4	In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to an incorrect bounds check. This could	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253424924References: N/A **CVE ID : CVE-2023-21046**	/pixel/2023-03-01	
Use After Free	24-Mar-2023	4.4	When cpif handles probe failures, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323725References: N/A **CVE ID : CVE-2023-21045**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3474
Out-of-bounds Read	24-Mar-2023	4.4	In append_camera_metadata of camera_metadata.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-236688120References: N/A **CVE ID : CVE-2023-21049**		
Out-of-bounds Read	24-Mar-2023	4.4	In handleEvent of nan.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259304053References: N/A **CVE ID : CVE-2023-21048**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3476
Affected Version(s): 11.0					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-258652631 **CVE ID : CVE-2023-20951**		
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 **CVE ID : CVE-2023-20954**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3478
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-221040577 **CVE ID : CVE-2023-20906**		
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 **CVE ID : CVE-2023-20911**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3480
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file 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-11 Android-12 Android-12L Android-13Android ID: A-242605257	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20917		
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 **CVE ID : CVE-2023-20931**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3482
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.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-11 Android-12 Android-12L Android-13Android ID: A-226927612 **CVE ID : CVE-2023-20936**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3483
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of	https://source.android.com/secur	O-GOO-ANDR-050423/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users 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-11 Android-12 Android-12L Android-13Android ID: A-258653813 **CVE ID : CVE-2023-20955**	ity/bulletin/2023-03-01	
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561 **CVE ID : CVE-2023-20957**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 **CVE ID : CVE-2023-20963**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3486
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736 **CVE ID : CVE-2023-20966**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3487
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 **CVE ID : CVE-2023-20910**		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 **CVE ID : CVE-2023-20952**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3489
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application with specific conditions. **CVE ID : CVE-2023-21463**		
Affected Version(s): 12.0					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 **CVE ID : CVE-2023-20951**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3491
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 **CVE ID : CVE-2023-20954**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577 **CVE ID : CVE-2023-20906**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3493
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20911		
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file 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-11 Android-12 Android-12L Android-13Android ID: A-242605257 **CVE ID : CVE-2023-20917**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3495
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 **CVE ID : CVE-2023-20931**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.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-11 Android-12 Android-12L Android-13Android ID: A-226927612 **CVE ID : CVE-2023-20936**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3497
N/A	24-Mar-2023	7.8	In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted 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-12 Android-12L Android-13Android ID: A-237405974 **CVE ID : CVE-2023-20947**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3498
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin restrictions and uninstall applications for all users 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-11 Android-12 Android-12L Android-13Android ID: A-258653813 **CVE ID : CVE-2023-20955**	/2023-03-01	
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561 **CVE ID : CVE-2023-20957**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3500
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 **CVE ID : CVE-2023-20963**	/2023-03-01	
N/A	24-Mar-2023	7.8	In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 **CVE ID : CVE-2023-20964**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3502
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-242299736 **CVE ID : CVE-2023-20966**		
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 **CVE ID : CVE-2023-20926**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3504
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS 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-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-245299920 **CVE ID : CVE-2023-20910**		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 **CVE ID : CVE-2023-20952**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3506
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240140929 **CVE ID : CVE-2023-20956**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. **CVE ID : CVE-2023-21462**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3508
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. **CVE ID : CVE-2023-21463**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3509
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. **CVE ID : CVE-2023-21464**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3510
Affected Version(s): 12.1					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 **CVE ID : CVE-2023-20951**	/2023-03-01	
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 **CVE ID : CVE-2023-20954**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3512
Improper Input Validation	24-Mar-2023	8.8	In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-250589026 **CVE ID : CVE-2023-20960**		
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577 **CVE ID : CVE-2023-20906**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3514
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 **CVE ID : CVE-2023-20911**		
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file 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-11 Android-12 Android-12L Android-13Android ID: A-242605257 **CVE ID : CVE-2023-20917**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3516
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. 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/2023-03-01	O-GOO-ANDR-050423/3517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 **CVE ID : CVE-2023-20931**		
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.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-11 Android-12 Android-12L Android-13Android ID: A-226927612 **CVE ID : CVE-2023-20936**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3518
N/A	24-Mar-2023	7.8	In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted 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-12 Android-12L Android-13Android ID: A-237405974	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20947		
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users 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-11 Android-12 Android-12L Android-13Android ID: A-258653813 **CVE ID : CVE-2023-20955**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3520
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20957		
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 **CVE ID : CVE-2023-20963**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3522
N/A	24-Mar-2023	7.8	In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 **CVE ID : CVE-2023-20964**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3523
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3524

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-11 Android-12 Android-12L Android-13Android ID: A-242299736 **CVE ID : CVE-2023-20966**		
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 **CVE ID : CVE-2023-20926**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3525
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 **CVE ID : CVE-2023-20910**		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 **CVE ID : CVE-2023-20952**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3527
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-240140929 **CVE ID : CVE-2023-20956**		
Affected Version(s): 13.0					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 **CVE ID : CVE-2023-20951**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3529
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20954		
Improper Input Validation	24-Mar-2023	8.8	In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-250589026 **CVE ID : CVE-2023-20960**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3531
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass 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-13Android ID: A-261193711 **CVE ID : CVE-2023-21003**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 **CVE ID : CVE-2023-20911**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3533
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file 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-11 Android-12 Android-12L Android-13Android ID: A-242605257 **CVE ID : CVE-2023-20917**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3534
N/A	24-Mar-2023	7.8	In InstallStart of InstallStart.java, there is a possible way to change the installer package	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name due to an improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236687884 **CVE ID : CVE-2023-21017**	/pixel/2023-03-01	
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass 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-13Android ID: A-244569778 **CVE ID : CVE-2023-21015**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3536
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 **CVE ID : CVE-2023-20931**		
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.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-11 Android-12 Android-12L Android-13Android ID: A-226927612 **CVE ID : CVE-2023-20936**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3538
N/A	24-Mar-2023	7.8	In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted 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-12 Android-12L Android-13Android ID: A-237405974	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20947		
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass 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-13Android ID: A-261193946 **CVE ID : CVE-2023-21005**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3540
N/A	24-Mar-2023	7.8	In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to bypass factory reset protection due to incorrect UI being shown prior to setup completion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251778420 **CVE ID : CVE-2023-20953**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users 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-11 Android-12 Android-12L Android-13Android ID: A-258653813 **CVE ID : CVE-2023-20955**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3542
Out-of-bounds Write	24-Mar-2023	7.8	In BTA_GATTS_HandleValueIndication of bta_gatts_api.cc, there is a possible out of bounds write due to improper input validation. This could 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-245915315 **CVE ID : CVE-2023-20985**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass 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-13Android ID: A-261193664 **CVE ID : CVE-2023-21004**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3544
Missing Authorization	24-Mar-2023	7.8	In AddSupervisedUserActivity, guest users are not prevented from starting the activity due to missing permissions checks. This could 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-249057848 **CVE ID : CVE-2023-20959**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3545
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577 **CVE ID : CVE-2023-20906**		
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass 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-13Android ID: A-261193935 **CVE ID : CVE-2023-21002**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3547
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. 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/2023-03-01	O-GOO-ANDR-050423/3548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 **CVE ID : CVE-2023-20963**		
N/A	24-Mar-2023	7.8	In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 **CVE ID : CVE-2023-20964**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3549
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20966		
Missing Authorization	24-Mar-2023	7.8	In onContextItemSelected of NetworkProviderSettings.java, there is a possible way for users to change the Wi-Fi settings of other users 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-13Android ID: A-237672190 **CVE ID : CVE-2023-21001**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3551
Improper Locking	24-Mar-2023	7.8	In MediaCodec.cpp, there is a possible use after free due to improper locking. This could 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-194783918 **CVE ID : CVE-2023-21000**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3552
N/A	24-Mar-2023	7.8	In captureImage of CustomizedSensor.cpp, there is a possible way to bypass the fingerprint unlock due to a logic	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-13Android ID: A-241910279 **CVE ID : CVE-2023-20995**	/pixel/2023-03-01	
N/A	24-Mar-2023	7.8	In updatePermissionTreeSourcePackage of PermissionManagerServiceImpl.java, there is a possible way to obtain dangerous permission without the user's consent 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-13Android ID: A-225880325 **CVE ID : CVE-2023-20971**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3554
Improper Handling of Exceptional Conditions	24-Mar-2023	7.8	In multiple functions of SnoozeHelper.java, there is a possible failure to persist settings due to an uncaught exception. This could lead to local escalation of privilege with no additional	N/A	O-GOO-ANDR-050423/3555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261588851 **CVE ID : CVE-2023-20993**		
Incorrect Authorization	24-Mar-2023	7.8	In multiple functions of BackupHelper.java, there is a possible way for an app to get permissions previously granted to another app with the same package name 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-13Android ID: A-184847040 **CVE ID : CVE-2023-21035**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3556
Incorrect Authorization	24-Mar-2023	7.8	In multiple functions of SensorService.cpp, there is a possible access of accurate sensor data due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-230358834 **CVE ID : CVE-2023-21034**		
N/A	24-Mar-2023	7.8	In getAvailabilityStatus of EnableContentCapturePreferenceController.java, there is a possible way to bypass DISALLOW_CONTENT_CAPTURE 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-13Android ID: A-250573776 **CVE ID : CVE-2023-20975**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3558
Double Free	24-Mar-2023	7.8	In Confirmation of keystore_cli_v2.cpp, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226234140 **CVE ID : CVE-2023-21030**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Mar-2023	7.8	In maybeFinish of FallbackHome.java, there is a possible delay of lockdown screen due to logic error. This could 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-246543238 **CVE ID : CVE-2023-21024**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3560
Out-of-bounds Write	24-Mar-2023	7.8	In BufferBlock of Suballocation.cpp, there is a possible out of bounds write due to memory corruption. This could 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-236098131 **CVE ID : CVE-2023-21022**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3561
Missing Authorization	24-Mar-2023	7.8	In isTargetSdkLessThanQOrPrivileged of WifiServiceImpl.java, there is a possible way for the guest user to change admin user network settings due to a missing permission check. This could lead to	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3562

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.Product: AndroidVersions: Android-13Android ID: A-255537598 **CVE ID : CVE-2023-21021**		
Out-of-bounds Read	24-Mar-2023	7.5	In parse_printerAttributes of ipphelper.c, there is a possible out of bounds read due to a string without a null-terminator. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-180680572 **CVE ID : CVE-2023-21028**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3563
N/A	24-Mar-2023	7.5	In serializePasspointConfiguration of PasspointXmlUtils.java, there is a possible logic error in the code. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-13Android ID: A-216854451 **CVE ID : CVE-2023-21027**		
Improper Input Validation	24-Mar-2023	7.3	In getConfirmationMessage of DefaultAutofillPicker.java , there is a possible way to mislead the user to select default autofill application due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-216117246 **CVE ID : CVE-2023-20976**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3565
Out-of-bounds Read	24-Mar-2023	7.1	In read_paint of ttcolr.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254803162 **CVE ID : CVE-2023-20958**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 **CVE ID : CVE-2023-20926**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3567
Out-of-bounds Write	24-Mar-2023	6.7	In _ufdt_output_property_to_fdt of ufdt_convert.c, 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.Product: AndroidVersions: Android-13Android ID: A-259062118 **CVE ID : CVE-2023-20994**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3568
Use After Free	24-Mar-2023	6.7	In UnwindingWorker of unwinding.cc, there is a possible out of bounds write due to a use after	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233338564 **CVE ID : CVE-2023-21018**	/pixel/2023-03-01	
Use After Free	24-Mar-2023	6.7	In registerSignalHandlers of main.c, there is a possible local arbitrary code execution due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256591441 **CVE ID : CVE-2023-21020**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3570
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS 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-11 Android-12	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12L Android-13Android ID: A-245299920 **CVE ID : CVE-2023-20910**		
N/A	24-Mar-2023	5.5	In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700 **CVE ID : CVE-2023-20929**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3572
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-186803518 **CVE ID : CVE-2023-20952**		
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936 **CVE ID : CVE-2023-20998**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3574
N/A	24-Mar-2023	5.5	In getSliceEndItem of MediaVolumePreferenceController.java, there is a possible way to start foreground activity from the background due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256590210 **CVE ID : CVE-2023-20962**	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3575
Loop with Unreachabl	24-Mar-2023	5.5	In multiple locations, there is a possible way to	https://source.android	O-GOO-ANDR-050423/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467 **CVE ID : CVE-2023-20999**	.com/security/bulletin/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884 **CVE ID : CVE-2023-21016**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3577
Improper Restriction of Operations within the Bounds of	24-Mar-2023	5.5	In btm_vendor_specific_evt of btm_devctl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304665 **CVE ID : CVE-2023-20972**		
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749764 **CVE ID : CVE-2023-20996**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3579
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749702	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20997		
Out-of-bounds Read	24-Mar-2023	5.5	In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731 **CVE ID : CVE-2023-21019**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3581
Out-of-bounds Read	24-Mar-2023	5.5	In btu_ble_ll_conn_param_upd_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260230274 **CVE ID : CVE-2023-20980**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3582
Out-of-bounds Read	24-Mar-2023	5.5	In BtaAvCo::GetNextSourceDataPacket of bta_av_co.cc, there is a possible out of bounds	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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.Product: AndroidVersions: Android-13Android ID: A-259939364 **CVE ID : CVE-2023-20979**	/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254681548 **CVE ID : CVE-2023-21026**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3584
Missing Authorization	24-Mar-2023	5.5	In register of UidObserverController.java, there is a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-217934898 **CVE ID : CVE-2023-21029**		
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetwork of WifiManager.java, there is a possible way to trigger a persistent DoS 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-13Android ID: A-244713323 **CVE ID : CVE-2023-21033**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3586
Out-of-bounds Read	24-Mar-2023	5.5	In btm_ble_add_resolving_list_entry_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260078907 **CVE ID : CVE-2023-20974**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3587
Out-of-bounds Read	24-Mar-2023	5.5	In btm_create_conn_cancel_complete of btm_sec.cc,	https://source.android.com/secur	O-GOO-ANDR-050423/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568245 **CVE ID : CVE-2023-20973**	ity/bulletin/pixel/2023-03-01	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	24-Mar-2023	4.7	In Display::setPowerMode of HWC2.cpp, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242688355 **CVE ID : CVE-2023-21031**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3589
Out-of-bounds Read	24-Mar-2023	4.5	In btm_read_rssi_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569232 **CVE ID : CVE-2023-20988**		
Out-of-bounds Read	24-Mar-2023	4.5	In btm_read_link_quality_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569414 **CVE ID : CVE-2023-20987**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3591
Out-of-bounds Read	24-Mar-2023	4.5	In on_iso_link_quality_read of btm_iso_impl.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568750 **CVE ID : CVE-2023-20992**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029912 **CVE ID : CVE-2023-21011**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3593
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029812 **CVE ID : CVE-2023-21012**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3594
Out-of-bounds Read	24-Mar-2023	4.4	In forceStaDisconnection of hostapd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-13Android ID: A-256818945 **CVE ID : CVE-2023-21013**		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029326 **CVE ID : CVE-2023-21014**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3596
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_rand_enc_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569449 **CVE ID : CVE-2023-20983**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3597
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029915 **CVE ID : CVE-2023-21010**	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In btm_read_tx_power_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568083 **CVE ID : CVE-2023-20982**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3599
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L	https://source.android.com/security/bulletin/2023-03-01	O-GOO-ANDR-050423/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-240140929 **CVE ID : CVE-2023-20956**		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235935 **CVE ID : CVE-2023-20968**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3601
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236313 **CVE ID : CVE-2023-20969**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3602
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236005 **CVE ID : CVE-2023-20970**		
Out-of-bounds Read	24-Mar-2023	4.4	In btm_read_local_oob_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568354 **CVE ID : CVE-2023-20990**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3604
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_read_remote_features_complete of btm_ble_gap.cc, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-254445952 **CVE ID : CVE-2023-20977**		
Out-of-bounds Read	24-Mar-2023	4.4	In ufdt_local_fixup_prop of ufdt_overlay.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254929746 **CVE ID : CVE-2023-21025**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3606
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_write_adv_enable_complete of btm_ble_gap.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568367 **CVE ID : CVE-2023-20989**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3607
Out-of-bounds Read	24-Mar-2023	4.4	In btu_ble_rc_param_req_evt of btu_hcif.cc, there is a possible out of bounds	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256165737 **CVE ID : CVE-2023-20981**	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_process_periodic_adv_sync_lost_evt of ble_scanner_hci_interface.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255305114 **CVE ID : CVE-2023-20991**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3609
Out-of-bounds Read	24-Mar-2023	4.4	In ParseBqrLinkQualityEvt of btif_bqr.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-13Android ID: A-242993878 **CVE ID : CVE-2023-20984**		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030027 **CVE ID : CVE-2023-21006**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3611
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029965 **CVE ID : CVE-2023-21007**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3612
Out-of-bounds Read	24-Mar-2023	4.4	In _ufdt_output_node_to_fdt of ufdt_convert.c, there is a possible out of bounds read due to a heap buffer	https://source.android.com/security/bulletin	O-GOO-ANDR-050423/3613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-248085351 **CVE ID : CVE-2023-21032**	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030100 **CVE ID : CVE-2023-21008**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3614
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029925	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21009		
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_clear_resolving_list_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304475 **CVE ID : CVE-2023-20986**	https://source.android.com/security/bulletin/pixel/2023-03-01	O-GOO-ANDR-050423/3616
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. **CVE ID : CVE-2023-21462**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3617
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application with specific conditions. **CVE ID : CVE-2023-21463**		
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. **CVE ID : CVE-2023-21464**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=03	O-GOO-ANDR-050423/3619
Vendor: hgiga					
Product: powerstation_firmware					
Affected Version(s): * Up to (excluding) x64.6.2.165					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	8.8	HGiga PowerStation remote management function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service. **CVE ID : CVE-2023-24837**	https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html	O-HGI-POWE-050423/3620
Missing Authentication for Critical Function	27-Mar-2023	7.5	HGiga PowerStation has a vulnerability of Information Leakage. An unauthenticated remote attacker can exploit this vulnerability to obtain the administrator's credential, resulting in performing arbitrary	https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html	O-HGI-POWE-050423/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system operation or disrupt service. **CVE ID : CVE-2023-24838**		
Vendor: HP					
Product: integrated_lights-out_4					
Affected Version(s): * Up to (excluding) 2.82					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	O-HP-INTE-050423/3622
Product: integrated_lights-out_5					
Affected Version(s): * Up to (excluding) 2.78					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	O-HP-INTE-050423/3623
Product: integrated_lights-out_6					
Affected Version(s): * Up to (excluding) 1.20					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. **CVE ID : CVE-2023-28083**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	O-HP-INTE-050423/3624
Vendor: hpe					
Product: arubaos-cx					
Affected Version(s): From (including) 10.06.0000 Up to (excluding) 10.06.0240					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	O-HPE-ARUB-050423/3625
Affected Version(s): From (including) 10.08.0000 Up to (including) 10.08.1070					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	O-HPE-ARUB-050423/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**		
Affected Version(s): From (including) 10.09.0000 Up to (including) 10.09.1020					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. **CVE ID : CVE-2023-1168**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	O-HPE-ARUB-050423/3627
Affected Version(s): From (including) 10.10.0000 Up to (excluding) 10.10.1030					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt	O-HPE-ARUB-050423/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1168		
Vendor: jcgcn.com					
Product: jhr-n916r_firmware					
Affected Version(s): * Up to (including) 21.11.1.1483					
N/A	16-Mar-2023	9.8	Command execution vulnerability was discovered in JHR-N916R router firmware version<=21.11.1.1483. **CVE ID : CVE-2023-24795**	N/A	O-JCG-JHR--050423/3629
Vendor: lancombg					
Product: sa-wr915nd_firmware					
Affected Version(s): 17.35.1					
N/A	16-Mar-2023	9.8	SA-WR915ND router firmware v17.35.1 was discovered to be vulnerable to code execution. **CVE ID : CVE-2023-23150**	N/A	O-LAN-SA-W-050423/3630
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must	https://success.trendmicro.com/solution/000292486	O-LIN-LINU-050423/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			first obtain a low-privileged authenticated user's profile on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-25069**		
Improper Restriction of XML External Entity Reference	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845. **CVE ID : CVE-2023-27874**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249845	O-LIN-LINU-050423/3632
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-25590**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	O-LIN-LINU-050423/3633
Improper Neutralization of Special Elements used in an SQL Command	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.	O-LIN-LINU-050423/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			query. IBM X-Force ID: 249613. **CVE ID : CVE-2023-27871**	com/vulnerabilities/249613	
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. **CVE ID : CVE-2023-27875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249847, https://www.ibm.com/support/pages/node/6963662	O-LIN-LINU-050423/3635
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. **CVE ID : CVE-2023-27873**	https://www.ibm.com/support/pages/node/6964694, https://exchange.xforce.ibmcloud.com/vulnerabilities/249654	O-LIN-LINU-050423/3636
Affected Version(s): * Up to (excluding) 5.11					
N/A	16-Mar-2023	7.5	A remote denial of service vulnerability was found in the Linux kernel's TIPC kernel module. The while loop in tipc_link_xmit() hits an unknown state while attempting to parse SKBs, which are not in the queue. Sending two small UDP packets to a system with a UDP bearer results in the CPU utilization for the system to instantly spike to 100%, causing a	https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6, https://infosec.exchange/@_mattata/109427999461122360	O-LIN-LINU-050423/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition. **CVE ID : CVE-2023-1390**		
Affected Version(s): * Up to (excluding) 5.13.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-2023	7.8	An issue was discovered in the Linux kernel before 5.13.3. lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow. **CVE ID : CVE-2023-28772**	https://github.com/torvalds/linux/commit/d3b16034a24a112bb83aeb669ac5b9b01f744bb7, https://lkml.kernel.org/r/20210626032156.47889-1-yun.zhou@windriver.com, https://lore.kernel.org/lkml/20210625122453.5e2fe304@oasis.local.home/	O-LIN-LINU-050423/3638
Affected Version(s): * Up to (excluding) 5.16					
Use After Free	23-Mar-2023	7.8	A use-after-free flaw was found in the Linux kernel's Ext4 File System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local user to crash or potentially escalate their privileges on the system. Only if patch 9a2544037600 ("ovl: fix use after free in	https://lore.kernel.org/lkml/20211115165433.44995128 5@linuxfoundation.org/	O-LIN-LINU-050423/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			struct ovl_aio_req") not applied yet, the kernel could be affected. **CVE ID : CVE-2023-1252**		
Affected Version(s): * Up to (excluding) 5.18					
Use After Free	23-Mar-2023	5.5	A use-after-free flaw was found in the Linux kernel's core dump subsystem. This flaw allows a local user to crash the system. Only if patch 390031c94211 ("coredump: Use the vma snapshot in fill_files_note") not applied yet, then kernel could be affected. **CVE ID : CVE-2023-1249**	https://patchwork.kernel.org/project/linux-fsdevel/patch/87iltzn3nd.fsf_-_@email.froward.int.ebiederm.org/	O-LIN-LINU-050423/3640
Affected Version(s): * Up to (excluding) 6.1					
Use After Free	23-Mar-2023	4.7	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. **CVE ID : CVE-2023-0590**	https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/	O-LIN-LINU-050423/3641
Affected Version(s): * Up to (excluding) 6.2					
N/A	22-Mar-2023	7.8	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?i	O-LIN-LINU-050423/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. **CVE ID : CVE-2023-0386**	d=4f11ada10d0a	
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	27-Mar-2023	6.8	A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the work_struct may be scheduled by the LED controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A malicious USB device may exploit the issue to cause memory corruption with controlled data. **CVE ID : CVE-2023-1079**	https://git.kernel.org/pub/scm/linux/kernel/git/next/linux-next.git/commit/?id=4ab3a086d10eeec1424f2e8a968827a6336203df	O-LIN-LINU-050423/3643
Affected Version(s): * Up to (including) 6.2.6					
NULL Pointer Dereference	16-Mar-2023	7	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (with a resultant use-after-free	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id	O-LIN-LINU-050423/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or NULL pointer dereference). **CVE ID : CVE-2023-28466**	=49c47cc21b5b7a3d8deb18fc57b0aa2ab1286962	
Affected Version(s): 5.11					
N/A	16-Mar-2023	7.5	A remote denial of service vulnerability was found in the Linux kernel's TIPC kernel module. The while loop in tipc_link_xmit() hits an unknown state while attempting to parse SKBs, which are not in the queue. Sending two small UDP packets to a system with a UDP bearer results in the CPU utilization for the system to instantly spike to 100%, causing a denial of service condition. **CVE ID : CVE-2023-1390**	https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6, https://infosec.exchange/@_mattata/109427999461122360	O-LIN-LINU-050423/3645
Affected Version(s): 5.19					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An	https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&id=761efd55a0227aca3a69deacdaa112fffd44fe37	O-LIN-LINU-050423/3646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged user can use the flaw to cause a system crash. **CVE ID : CVE-2023-1583**		
Affected Version(s): 6.0					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. **CVE ID : CVE-2023-1583**	https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&id=761efd55a0227aca3a69deacdaa112fffd44fe37	O-LIN-LINU-050423/3647
Affected Version(s): 6.1					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL	https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&id=761efd55a0227aca3a69deacdaa112fffd44fe37	O-LIN-LINU-050423/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. **CVE ID : CVE-2023-1583**		
Use After Free	23-Mar-2023	4.7	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. **CVE ID : CVE-2023-0590**	https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/	O-LIN-LINU-050423/3649
Affected Version(s): 6.2					
N/A	22-Mar-2023	7.8	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. **CVE ID : CVE-2023-0386**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a	O-LIN-LINU-050423/3650
Use After Free	22-Mar-2023	7.8	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git	O-LIN-LINU-050423/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2. **CVE ID : CVE-2023-1281**	/commit/?id=ee059170b1f7e94e55fa6cadee544e176a6e59c2, https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2	
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. **CVE ID : CVE-2023-1583**	https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&id=761efd55a0227aca3a69deacdaa112fffd44fe37	O-LIN-LINU-050423/3652
Affected Version(s): 6.3					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the	https://git.kernel.org/pub/scm/linux/kernel	O-LIN-LINU-050423/3653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. **CVE ID : CVE-2023-1583**	/git/axboe/linux-block.git/commit/?h=io_uring-6.3&id=761efd55a0227aca3a69deacdaa112fffd44fe37	
Affected Version(s): From (including) 4.14 Up to (excluding) 6.2					
Use After Free	22-Mar-2023	7.8	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2. **CVE ID : CVE-2023-1281**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ee059170b1f7e94e55fa6cadee544e176a6e59c2, https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2	O-LIN-LINU-050423/3654
Vendor: Microsoft					
Product: windows					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Unquoted Search Path or Element	16-Mar-2023	7.8	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file. **CVE ID : CVE-2023-24671**	N/A	O-MIC-WIND-050423/3655
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25859**	https://helpx.adobe.com/security/products/illustrator/apsb23-19.html	O-MIC-WIND-050423/3656
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-25903**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26334**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3658
Out-of-bounds Read	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26335**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3659
Use After Free	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26336**		
Out-of-bounds Write	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26337**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3661
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. **CVE ID : CVE-2023-27875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249847, https://www.ibm.com/support/pages/node/6963662	O-MIC-WIND-050423/3662
N/A	22-Mar-2023	6.8	A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows? Secure Boot process in an	https://success.trendmicro.com/solution/000292473	O-MIC-WIND-050423/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to execute other attacks to obtain access to the contents of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone. **CVE ID : CVE-2023-28005**		
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26338**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3664
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	https://helpx.adobe.com/security/products/dimension/	O-MIC-WIND-050423/3665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26339**	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26340**	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	O-MIC-WIND-050423/3666
Vendor: Mikrotik					
Product: routeros					
Affected Version(s): 6.40.5					
Out-of-bounds Write	27-Mar-2023	7.5	An issue in the bridge2 component of MikroTik RouterOS v6.40.5 allows attackers to cause a Denial of Service (DoS) via crafted packets. **CVE ID : CVE-2023-24094**	N/A	O-MIK-ROUT-050423/3667
Vendor: Omron					
Product: sysmac_cj2h-cpu64-eip_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3668
Product: sysmac_cj2h-cpu64_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu65-eip_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3670
Product: sysmac_cj2h-cpu65_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu66-eip_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3672
Product: sysmac_cj2h-cpu66_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2h-cpu67-eip_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3674
Product: sysmac_cj2h-cpu67_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cj2h-cpu68-eip_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3676
Product: sysmac_cj2h-cpu68_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3677
Product: sysmac_cj2m-cpu11_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu12_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3679
Product: sysmac_cj2m-cpu13_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu14_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3681
Product: sysmac_cj2m-cpu15_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cj2m-cpu31_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3683
Product: sysmac_cj2m-cpu32_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cj2m-cpu33_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3685
Product: sysmac_cj2m-cpu34_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3686
Product: sysmac_cj2m-cpu35_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e10dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3688
Product: sysmac_cp1e-e10dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e10dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3690
Product: sysmac_cp1e-e10dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e10dt1-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3692
Product: sysmac_cp1e-e10dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1e-e14dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3694
Product: sysmac_cp1e-e14sdr-a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3695
Product: sysmac_cp1e-e20dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e20sdr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3697
Product: sysmac_cp1e-e30dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e30sdr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3699
Product: sysmac_cp1e-e40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1e-e40sdr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3701
Product: sysmac_cp1e-e60sdr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1e-na20dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3703
Product: sysmac_cp1e-na20dt-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3704
Product: sysmac_cp1e-na20dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1h-x40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3706
Product: sysmac_cp1h-x40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1h-x40dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3708
Product: sysmac_cp1h-xa40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1h-xa40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3710
Product: sysmac_cp1h-xa40dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1h-y20dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3712
Product: sysmac_cp1l-el20dr-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3713
Product: sysmac_cp1l-em30dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-em30dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3715
Product: sysmac_cp1l-em30dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-em40dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3717
Product: sysmac_cp1l-em40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-em40dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3719
Product: sysmac_cp1l-l10dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-l10dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3721
Product: sysmac_cp1l-l10dt-a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3722
Product: sysmac_cp1l-l10dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l10dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3724
Product: sysmac_cp1l-l14dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l14dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3726
Product: sysmac_cp1l-l14dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l14dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3728
Product: sysmac_cp1l-l14dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-l20dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3730
Product: sysmac_cp1l-l20dr-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3731
Product: sysmac_cp1l-l20dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-l20dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3733
Product: sysmac_cp1l-l20dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m30dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3735
Product: sysmac_cp1l-m30dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m30dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3737
Product: sysmac_cp1l-m30dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-m30dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3739
Product: sysmac_cp1l-m40dr-a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3740
Product: sysmac_cp1l-m40dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m40dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3742
Product: sysmac_cp1l-m40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m40dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3744
Product: sysmac_cp1l-m60dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp1l-m60dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3746
Product: sysmac_cp1l-m60dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp1l-m60dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3748
Product: sysmac_cp1l-m60dt1-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3749
Product: sysmac_cp2e-e14dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-e20dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3751
Product: sysmac_cp2e-e30dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-e40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3753
Product: sysmac_cp2e-e60dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n14dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3755
Product: sysmac_cp2e-n14dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n14dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3757
Product: sysmac_cp2e-n14dt-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3758
Product: sysmac_cp2e-n14dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n20dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3760
Product: sysmac_cp2e-n20dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n20dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3762
Product: sysmac_cp2e-n20dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n20dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3764
Product: sysmac_cp2e-n30dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n30dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3766
Product: sysmac_cp2e-n30dt-a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3767
Product: sysmac_cp2e-n30dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n30dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3769
Product: sysmac_cp2e-n40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n40dr-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3771
Product: sysmac_cp2e-n40dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3773
Product: sysmac_cp2e-n40dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-n60dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3775
Product: sysmac_cp2e-n60dr-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3776
Product: sysmac_cp2e-n60dt-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-n60dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3778
Product: sysmac_cp2e-n60dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s30dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3780
Product: sysmac_cp2e-s30dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s30dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3782
Product: sysmac_cp2e-s40dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cp2e-s40dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3784
Product: sysmac_cp2e-s40dt1-d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3785
Product: sysmac_cp2e-s60dr-a_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cp2e-s60dt-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3787
Product: sysmac_cp2e-s60dt1-d_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cs1w-drm21-v1_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3789
Product: sysmac_cs1w-eip21_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**		
Product: sysmac_cs1w-etn21_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3791
Product: sysmac_cs1w-fln22_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	https://www.ia.omron.com/produ	O-OMR-SYSM-050423/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	ct/vulnerability/OMSR-2023-001_en.pdf	
Product: sysmac_cs1w-nc\[\]71_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3793
Product: sysmac_cs1w-spu01-v2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. **CVE ID : CVE-2023-0811**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3794
Product: sysmac_cs1w-spu02-v2_firmware					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf	O-OMR-SYSM-050423/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the user program. **CVE ID : CVE-2023-0811**		
Vendor: paradox					
Product: ipr512_firmware					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	7.5	An issue found in Paradox Security Systems IPR512 allows attackers to cause a denial of service via the login.html and login.xml parameters. **CVE ID : CVE-2023-24709**	N/A	O-PAR-IPR5-050423/3796
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3797
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file	https://github.com/ImageMagick/ImageMa	O-RED-ENTE-050423/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	gick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bugzilla.redhat.com/show_bug.cgi?id=2176858	
Affected Version(s): 8.1					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-	O-RED-ENTE-050423/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	February/003320.html	
Affected Version(s): 9.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3800
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a	https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4, https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr, https://bug	O-RED-ENTE-050423/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. **CVE ID : CVE-2023-1289**	zilla.redhat.com/show_bug.cgi?id=2176858	
Product: enterprise_linux_aus					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3802
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://list	O-RED-ENTE-050423/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	s.x.org/archives/xorg-announce/2023-February/003320.html	
Product: enterprise_linux_desktop					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3804
Product: enterprise_linux_eus					
Affected Version(s): 9.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/arc	O-RED-ENTE-050423/3805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	hives/xorg-announce/2023-February/003320.html	
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3806
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-	O-RED-ENTE-050423/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	February/003320.html	
Product: enterprise_linux_for_ibm_z_systems					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3808
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions.	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0494		
Product: enterprise_linux_for_ibm_z_systems_eus					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3810
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3811
Product: enterprise_linux_for_power_big_endian					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3812
Product: enterprise_linux_for_power_little_endian					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3813
Affected Version(s): 9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3814
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3815
Product: enterprise_linux_for_power_little_endian_eus					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling	https://gitlab.freedesktop.org/xor	O-RED-ENTE-050423/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	g/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3817
Product: enterprise_linux_for_scientific_computing					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c370	O-RED-ENTE-050423/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	71131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	
Product: enterprise_linux_server					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3819
Product: enterprise_linux_server_aus					
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo()	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a497	O-RED-ENTE-050423/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	90243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	
Product: enterprise_linux_server_for_power_little_endian_update_services_for_sap_solutions					
Affected Version(s): 8.1					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3821
Affected Version(s): 9.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo()	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf7	O-RED-ENTE-050423/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	1ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3823
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-	O-RED-ENTE-050423/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	announce/2023-February/003320.html	
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3825
Product: enterprise_linux_server_tus					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-	O-RED-ENTE-050423/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	February/003320.html	
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3827
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: enterprise_linux_server_update_services_for_sap_solutions					
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3829
Product: enterprise_linux_server_workstation					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. **CVE ID : CVE-2023-0494**	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3830
Vendor: Samsung					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: android					
Affected Version(s): 11.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. **CVE ID : CVE-2023-21459**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3831
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. **CVE ID : CVE-2023-21457**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3832
N/A	16-Mar-2023	5.5	Improper access control vulnerability in Call application prior to SMR Mar-2023 Release 1 allows local attackers to access sensitive information without proper permission. **CVE ID : CVE-2023-21449**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3833
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid. **CVE ID : CVE-2023-21456**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3834
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirm	https://security.samsungmobile.c	O-SAM-ANDR-050423/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Dialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. **CVE ID : CVE-2023-21461**	om/securityUpdate.smsb?year=2023&month=03	
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. **CVE ID : CVE-2023-21460**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3836
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. **CVE ID : CVE-2023-21452**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3837
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent. **CVE ID : CVE-2023-21458**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3838
N/A	16-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users	https://security.samsungmobile.com/securityUpdate.smsb?year=20	O-SAM-ANDR-050423/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			text history on the lockscreen. **CVE ID : CVE-2023-21454**	23&month=03	
Affected Version(s): 12.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. **CVE ID : CVE-2023-21459**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3840
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. **CVE ID : CVE-2023-21457**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3841
N/A	16-Mar-2023	5.5	Improper access control vulnerability in Call application prior to SMR Mar-2023 Release 1 allows local attackers to access sensitive information without proper permission. **CVE ID : CVE-2023-21449**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3842
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21456		
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirmDialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. **CVE ID : CVE-2023-21461**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3844
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. **CVE ID : CVE-2023-21460**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3845
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. **CVE ID : CVE-2023-21452**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3846
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent. **CVE ID : CVE-2023-21458**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users text history on the lockscreen. **CVE ID : CVE-2023-21454**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3848
Affected Version(s): 13.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. **CVE ID : CVE-2023-21459**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3849
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. **CVE ID : CVE-2023-21457**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3850
Improper Input Validation	16-Mar-2023	5.5	Improper input validation vulnerability in SoftSim TA prior to SMR Mar-2023 Release 1 allows local attackers access to protected data. **CVE ID : CVE-2023-21453**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3851
Improper Limitation of a Pathname to a Restricted	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access	https://security.samsungmobile.com/securityUpdate.smsb?year=20	O-SAM-ANDR-050423/3852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			arbitrary file with system uid. **CVE ID : CVE-2023-21456**	23&month=03	
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirm Dialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. **CVE ID : CVE-2023-21461**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3853
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. **CVE ID : CVE-2023-21460**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3854
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. **CVE ID : CVE-2023-21452**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3855
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21458		
N/A	16-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users text history on the lockscreen. **CVE ID : CVE-2023-21454**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-ANDR-050423/3857
Product: exynos_1080_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3858
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for Video Configuration Attribute. **CVE ID : CVE-2023-26497**		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3860
Product: exynos_980_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3862
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3863
Product: exynos_auto_t5123_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-050423/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	security-updates/	
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3865
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3866
Product: exynos_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	16-Mar-2023	9.1	Improper authorization implementation in Exynos baseband prior to SMR Mar-2023 Release 1 allows incorrect handling of unencrypted message. **CVE ID : CVE-2023-21455**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=03	O-SAM-EXYN-050423/3867
Product: exynos_modem_5123_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3868
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26497		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3870
Product: exynos_modem_5300_firmware					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26496**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3871
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123,	https://semiconductor.samsung.com/suppor	O-SAM-EXYN-050423/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. **CVE ID : CVE-2023-26497**	t/quality-support/product-security-updates/	
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. **CVE ID : CVE-2023-26498**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-050423/3873
Vendor: sauter-controls					
Product: ey-as525f001_firmware					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	27-Mar-2023	6.5	An authenticated malicious user could acquire the simple mail transfer protocol (SMTP) Password in cleartext format, despite it being protected and hidden behind asterisks. The attacker could then perform further attacks	N/A	O-SAU-EY-A-050423/3874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using the SMTP credentials. **CVE ID : CVE-2023-27927**		
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	An authenticated malicious user could successfully upload a malicious image could lead to a denial-of-service condition. **CVE ID : CVE-2023-28652**	N/A	O-SAU-EY-A-050423/3875
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could force all authenticated users, such as administrative users, to perform unauthorized actions by viewing the logs. This action would also grant the attacker privilege escalation. **CVE ID : CVE-2023-22300**	N/A	O-SAU-EY-A-050423/3876
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could provide a malicious link and trick an unsuspecting user into clicking on it. If clicked, the attacker could execute the malicious JavaScript (JS) payload in the target's security context. **CVE ID : CVE-2023-28650**	N/A	O-SAU-EY-A-050423/3877
Improper Neutralization of Input During	27-Mar-2023	5.4	A malicious user could leverage this vulnerability to escalate privileges or perform unauthorized actions in	N/A	O-SAU-EY-A-050423/3878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the context of the targeted privileged users. **CVE ID : CVE-2023-28655**		
Vendor: silabs					
Product: wireless_smart_ubiquitous_network_linux_border_router_firmware					
Affected Version(s): * Up to (including) 1.5.2					
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network. **CVE ID : CVE-2023-1262**	N/A	O-SIL-WIRE-050423/3879
Vendor: Tenda					
Product: ax3_firmware					
Affected Version(s): 16.03.12.11					
Out-of-bounds Write	24-Mar-2023	8.8	Tenda AX3 V16.03.12.11 is vulnerable to Buffer Overflow via /goform/SetFirewallCfg. **CVE ID : CVE-2023-27042**	N/A	O-TEN-AX3_-050423/3880
Product: g103_firmware					
Affected Version(s): 1.0.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	7.5	Command Injection vulnerability found in Tenda G103 v.1.0.05 allows an attacker to obtain sensitive information via a crafted package **CVE ID : CVE-2023-27079**	N/A	O-TEN-G103-050423/3881
Product: w20e_firmware					
Affected Version(s): 15.11.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6 (US_W20EV4.0br_v15.11.0.6(1068_1546_841)_CN_TDC) is vulnerable to Buffer Overflow via function formIPMacBindModify. **CVE ID : CVE-2023-26805**	N/A	O-TEN-W20E-050423/3882
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6(US_W20EV4.0br_v15.11.0.6(1068_1546_841 is vulnerable to Buffer Overflow via function formSetSysTime, **CVE ID : CVE-2023-26806**	N/A	O-TEN-W20E-050423/3883
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the enabled parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-27135**	N/A	O-TOT-A710-050423/3884
Vendor: Tp-link					
Product: tl-mr3020_firmware					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command	23-Mar-2023	9.8	A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a	N/A	O-TP--TL-M-050423/3885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			crafted request to the tftp endpoint. **CVE ID : CVE-2023-27078**		
Vendor: ui					
Product: edgerouter_x_firmware					
Affected Version(s): 2.0.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. This issue affects some unknown processing of the component NAT Configuration Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier VDB-223301 was assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. **CVE ID : CVE-2023-1456**	N/A	O-UI-EDGE-050423/3886
Improper Neutralization of Special Elements used in a Command ('Comman	25-Mar-2023	9.8	** DISPUTED ** A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. Affected is an unknown function of the component Static Routing	N/A	O-UI-EDGE-050423/3887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Configuration Handler. The manipulation of the argument next-hop-interface leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-223302 is the identifier assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. **CVE ID : CVE-2023-1457**		