National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Aug 2023 Vol. 10 No. 15

Table of Content

Vendor	Product	Page Number
mediatek	mt6771	1170
	mt6779	1174
	mt6781	1181
	mt6783	1189
	mt6785	1189
	mt6789	1195
	mt6833	1199
	mt6835	1207
	mt6853	1211
	mt6853t	1220
	mt6855	1226
	mt6873	1234
	mt6875	1242
	mt6877	1249
	mt6879	1258
	mt6880	1269
	mt6883	1270
	mt6885	1278
	mt6886	1285
	mt6889	1293
	mt6890	1300
	mt6891	1301
	mt6893	1308
	mt6895	1316
	mt6896	1328
	mt6980	1329
	mt6983	1329
	mt6985	1341
	mt6990	1349
	mt8167	1350
	mt8167s	1352
	mt8168	1354

Vendor	Product	Page Number
mediatek	mt8173	1356
	mt8175	1357
	mt8183	1357
	mt8185	1358
	mt8188	1361
	mt8195	1367
	mt8195z	1373
	mt8321	1373
	mt8362a	1377
	mt8365	1379
	mt8385	1381
	mt8395	1384
	mt8666	1388
	mt8667	1391
	mt8673	1392
	mt8675	1398
	mt8765	1400
	mt8766	1404
	mt8768	1407
	mt8781	1410
	mt8786	1415
	mt8788	1419
	mt8789	1422
	mt8791	1424
	mt8791t	1427
	mt8797	1431
	mt9010	1434
	mt9011	1435
	mt9012	1437
	mt9016	1439
	mt9020	1440
	mt9021	1441

Vendor	Product	Page Number
mediatek	mt9022	1443
	mt9030	1444
	mt9031	1446
	mt9032	1447
	mt9215	1448
	mt9216	1449
	mt9218	1450
	mt9220	1452
	mt9221	1453
	mt9222	1454
	mt9255	1456
	mt9256	1457
	mt9266	1458
	mt9269	1460
	mt9285	1461
	mt9286	1462
	mt9288	1463
	mt9600	1464
	mt9602	1465
	mt9610	1466
	mt9611	1468
	mt9612	1469
	mt9613	1470
	mt9615	1472
	mt9617	1473
	mt9618	1474
	mt9629	1476
	mt9630	1477
	mt9631	1478
	mt9632	1480
	mt9636	1481
	mt9638	1482

Vendor	Product	Page Number
Qualcomm	qcm2290	1661
	qcm4290	1662
	qcm4325	1663
	qcm4490	1663
	qcm6125	1663
	qcm6490	1664
	qcn6024	1665
	qcn7606	1666
	qcn9011	1667
	qcn9012	1667
	qcn9024	1668
	qcn9074	1668
	qcs2290	1671
	qcs405	1672
	qcs410	1673
	qcs4290	1675
	qcs4490	1676
	qcs603	1677
	qcs605	1677
	qcs610	1678
	qcs6125	1681
	qcs6490	1681
	qcs8155	1683
	qcx315	1683
	qm215	1684
	qrb5165	1685
	qrb5165m	1685
	qrb5165n	1686
	qsm8250	1686
	qsm8350	1687
	qts110	1688
	s820a	1688

Vendor	Product	Page Number
Qualcomm	sa4150p	1688
	sa4155p	1689
	sa415m	1690
	sa515m	1691
	sa6145p	1692
	sa6150p	1694
	sa6155	1697
	sa6155p	1698
	sa8145p	1701
	sa8150p	1703
	sa8155	1706
	sa8155p	1707
	sa8195p	1710
	sa8295p	1712
	sa8540p	1714
	sa9000p	1715
	sc8180x\+sdx55	1716
	sd205	1716
	sd210	1717
	sd212	1718
	sd429	1719
	sd439	1719
	sd450	1720
	sd460	1721
	sd480	1722
	sd625	1723
	sd626	1724
	sd632	1725
	sd660	1725
	sd662	1726
	sd665	1727
	sd670	1728

Vendor	Product	Page Number
Qualcomm	sd675	1729
	sd678	1730
	sd680	1731
	sd690_5g	1732
	sd695	1733
	sd710	1734
	sd720g	1735
	sd730	1736
	sd750g	1737
	sd765	1738
	sd765g	1739
	sd768g	1740
	sd778g	1741
	sd780g	1742
	sd7c	1743
	sd835	1744
	sd845	1745
	sd850	1745
	sd855	1746
	sd865_5g	1748
	sd870	1751
	sd888	1753
	sd888_5g	1754
	sda429w	1755
	sda845	1756
	sdm429w	1757
	sdm630	1757
	sdm845	1758
	sdx12	1758
	sdx24	1758
	sdx50m	1759
	sdx55	1760

Vendor	Product	Page Number
Qualcomm	sdx55m	1762
	sdx57m	1763
	sdx65	1764
	sdxr1	1764
	sdxr2_5g	1765
	sd_455	1767
	sd_636	1767
	sd_675	1768
	sd_8cx	1769
	sd_8cx_gen2	1769
	sd_8cx_gen3	1770
	sd_8_gen1_5g	1770
	sg4150p	1772
	sm4125	1772
	sm4350	1773
	sm4350-ac	1774
	sm4375	1774
	sm4450	1775
	sm6225	1775
	sm6225-ad	1776
	sm6250	1776
	sm6250p	1777
	sm6375	1777
	sm7250p	1778
	sm7315	1779
	sm7325p	1780
	sm8350	1781
	sm8350-ac	1781
	sm8450	1782
	sm8475	1782
	smart_audio_100_platform	1782
	snapdragon_855	1782

Vendor	Product	Page Number
Qualcomm	snapdragon_855\+\/860	1783
	snapdragon_865\+_5g	1783
	snapdragon_865_5g	1784
	snapdragon_870_5g	1786
	snapdragon_8_gen_1	1787
	snapdragon_ar2_gen_1_platform	1788
	snapdragon_auto_4g_modem	1789
	snapdragon_auto_5g_modem-rf	1789
	snapdragon_w5\+_gen_1	1789
	snapdragon_w5\+_gen_1_wearable_platform	1790
	snapdragon_wear_4100\+	1790
	snapdragon_wear_4100\+_platform	1790
	snapdragon_x12_lte_modem	1791
	snapdragon_x24_lte_modem	1791
	snapdragon_x50_5g_modem-rf_system	1791
	snapdragon_x55_5g	1791
	snapdragon_x55_5g_modem-rf_system	1793
	snapdragon_x65_5g_modem-rf_system	1793
	snapdragon_xr1_platform	1793
	snapdragon_xr2\+_gen_1_platform	1794
	snapdragon_xr2_5g	1794
	snapdragon_xr2_5g_platform	1795
	ssg2115p	1795
	ssg2125p	1796
	sw5100	1797
	sw5100p	1800
	sxr1120	1803
	sxr1230p	1803
	sxr2130	1803
	sxr2150p	1805
	sxr2230p	1806
	wcd9306	1806

Vendor	Product	Page Number
Asus	rt-ac66u_b1_firmware	1977
Broadcom	brocade_fabric_operating_system	1978
	fabric_operating_system	1982
Cisco	asyncos	1985
	spa500ds_firmware	2007
	spa500s_firmware	2009
	spa501g_firmware	2011
	spa502g_firmware	2013
	spa504g_firmware	2015
	spa508g_firmware	2017
	spa509g_firmware	2019
	spa512g_firmware	2021
	spa514g_firmware	2023
	spa525g2_firmware	2025
	spa525g_firmware	2027
	spa525_firmware	2030
connectedio	er2000t-vz-cat1_firmware	2032
Debian	debian_linux	2032
Emerson	dl8000_firmware	2041
	roc809l_firmware	2041
	roc809_firmware	2041
	roc827l_firmware	2042
	roc827_firmware	2042
Epson	ep-801a_firmware	2042
	ep-802a_firmware	2043
	ep-901a_firmware	2044
	ep-901f_firmware	2045
	ep-902a_firmware	2045
	pa-tcu1_firmware	2046
	pm-t960_firmware	2047
	pm-t990_firmware	2048
	px-201_firmware	2049

Vendor	Product	Page Number
Mitsubishielectric	m750vs_15-type_firmware	2251
	m750vs_firmware	2251
	m750vw_firmware	2252
	m800s_firmware	2252
	m800vs_firmware	2253
	m800vw_firmware	2254
	m800w_firmware	2254
	m80vw_firmware	2255
	m80v_firmware	2255
	m80w_firmware	2256
	m80_firmware	2256
Netgear	dc112a_firmware	2257
	dg834gv5_firmware	2257
	dgn3500_firmware	2258
	ex6200_firmware	2258
	jwnr2000v2_firmware	2258
	r6300v2_firmware	2259
	r6900p_firmware	2260
	r7100lg_firmware	2260
	wag302v2_firmware	2260
	wg302v2_firmware	2261
	xavn2001v2_firmware	2261
	xr300_firmware	2262
	xwn5001_firmware	2262
Omron	cj1w-eip21_firmware	2263
	cj2h-cpu64-eip_firmware	2264
	cj2h-cpu65-eip_firmware	2265
	cj2h-cpu66-eip_firmware	2266
	cj2h-cpu67-eip_firmware	2268
	cj2h-cpu68-eip_firmware	2269
	cj2m-cpu31_firmware	2270
	cj2m-cpu32_firmware	2271

Vendor	Product	Page Number
Omron	cj2m-cpu33_firmware	2272
	cj2m-cpu34_firmware	2273
	cj2m-cpu35_firmware	2274
	cs1w-eip21_firmware	2276
openwrt	openwrt	2277
oppo	coloros	2279
Phoenixcontact	cloud_client_1101t-tx_firmware	2279
	tc_cloud_client_1002-4g_att_firmware	2280
	tc_cloud_client_1002-4g_firmware	2281
	tc_cloud_client_1002-4g_vzw_firmware	2282
	tc_router_3002t-4g_att_firmware	2283
	tc_router_3002t-4g_firmware	2284
	tc_router_3002t-4g_vzw_firmware	2285
	wp_6070-wvps_firmware	2286
	wp_6101-wxps_firmware	2291
	wp_6121-wxps_firmware	2296
	wp_6156-whps_firmware	2302
	wp_6185-whps_firmware	2307
	wp_6215-whps_firmware	2312
Qualcomm	205_firmware	2318
	215_firmware	2318
	315_5g_iot_modem_firmware	2318
	8098_firmware	2319
	8998_firmware	2319
	apq5053-aa_firmware	2319
	apq8009_firmware	2319
	apq8017_firmware	2320
	apq8037_firmware	2321
	apq8053-aa_firmware	2322
	apq8053-ac_firmware	2322
	apq8064au_firmware	2322
	apq8096au_firmware	2322

Vendor	Product	Page Number
Qualcomm	aqt1000_firmware	2323
	ar8031_firmware	2325
	ar8035_firmware	2326
	c-v2x_9150_firmware	2327
	csra6620_firmware	2328
	csra6640_firmware	2329
	csrb31024_firmware	2330
	fastconnect_6200_firmware	2331
	fastconnect_6800_firmware	2331
	fastconnect_6900_firmware	2333
	fastconnect_7800_firmware	2334
	flight_rb5_5g_platform_firmware	2335
	fsm10056_firmware	2336
	mdm8207_firmware	2336
	mdm9205_firmware	2336
	mdm9206_firmware	2337
	mdm9207_firmware	2337
	mdm9250_firmware	2337
	mdm9607_firmware	2338
	mdm9628_firmware	2338
	mdm9650_firmware	2339
	msm8108_firmware	2339
	msm8208_firmware	2340
	msm8209_firmware	2341
	msm8608_firmware	2342
	msm8917_firmware	2343
	msm8920_firmware	2344
	msm8937_firmware	2344
	msm8940_firmware	2345
	msm8996au_firmware	2345
	pm8937_firmware	2345
	qam8295p_firmware	2346

Vendor	Product	Page Number
Qualcomm	qca4004_firmware	2348
	qca4010_firmware	2348
	qca4020_firmware	2349
	qca4024_firmware	2349
	qca6174a_firmware	2350
	qca6310_firmware	2351
	qca6320_firmware	2352
	qca6335_firmware	2352
	qca6390_firmware	2353
	qca6391_firmware	2355
	qca6420_firmware	2358
	qca6421_firmware	2360
	qca6426_firmware	2362
	qca6430_firmware	2365
	qca6431_firmware	2367
	qca6436_firmware	2368
	qca6554a_firmware	2371
	qca6564au_firmware	2371
	qca6564a_firmware	2373
	qca6564_firmware	2375
	qca6574au_firmware	2376
	qca6574a_firmware	2379
	qca6574_firmware	2381
	qca6584au_firmware	2382
	qca6595au_firmware	2383
	qca6595_firmware	2385
	qca6696_firmware	2387
	qca6698aq_firmware	2389
	qca8081_firmware	2390
	qca8337_firmware	2391
	qca9367_firmware	2393
	qca9377_firmware	2393

Vendor	Product	Page Number
Qualcomm	qca9379_firmware	2394
	qca9984_firmware	2395
	qcc5100_firmware	2395
	qcm2290_firmware	2397
	qcm4290_firmware	2398
	qcm4325_firmware	2399
	qcm4490_firmware	2399
	qcm6125_firmware	2399
	qcm6490_firmware	2400
	qcn6024_firmware	2401
	qcn7606_firmware	2402
	qcn9011_firmware	2403
	qcn9012_firmware	2403
	qcn9024_firmware	2404
	qcn9074_firmware	2404
	qcs2290_firmware	2407
	qcs405_firmware	2408
	qcs410_firmware	2409
	qcs4290_firmware	2411
	qcs4490_firmware	2412
	qcs603_firmware	2413
	qcs605_firmware	2413
	qcs610_firmware	2414
	qcs6125_firmware	2417
	qcs6490_firmware	2417
	qcs8155_firmware	2419
	qcx315_firmware	2419
	qm215_firmware	2420
	qrb5165m_firmware	2421
	qrb5165n_firmware	2421
	qrb5165_firmware	2422
	qsm8250_firmware	2422

Vendor	Product	Page Number
Qualcomm	qsm8350_firmware	2423
	qts110_firmware	2424
	s820a_firmware	2424
	sa4150p_firmware	2424
	sa4155p_firmware	2425
	sa415m_firmware	2426
	sa515m_firmware	2427
	sa6145p_firmware	2428
	sa6150p_firmware	2430
	sa6155p_firmware	2433
	sa6155_firmware	2435
	sa8145p_firmware	2437
	sa8150p_firmware	2439
	sa8155p_firmware	2442
	sa8155_firmware	2444
	sa8195p_firmware	2446
	sa8295p_firmware	2448
	sa8540p_firmware	2450
	sa9000p_firmware	2451
	sc8180x\+sdx55_firmware	2452
	sd205_firmware	2452
	sd210_firmware	2453
	sd212_firmware	2454
	sd429_firmware	2455
	sd439_firmware	2455
	sd450_firmware	2456
	sd460_firmware	2457
	sd480_firmware	2458
	sd625_firmware	2459
	sd626_firmware	2460
	sd632_firmware	2461
	sd660_firmware	2461

Vendor	Product	Page Number
Qualcomm	sd662_firmware	2462
	sd665_firmware	2463
	sd670_firmware	2464
	sd675_firmware	2465
	sd678_firmware	2466
	sd680_firmware	2467
	sd690_5g_firmware	2468
	sd695_firmware	2469
	sd710_firmware	2470
	sd720g_firmware	2471
	sd730_firmware	2472
	sd750g_firmware	2473
	sd765g_firmware	2474
	sd765_firmware	2475
	sd768g_firmware	2476
	sd778g_firmware	2477
	sd780g_firmware	2478
	sd7c_firmware	2479
	sd835_firmware	2480
	sd845_firmware	2481
	sd850_firmware	2481
	sd855_firmware	2482
	sd865_5g_firmware	2484
	sd870_firmware	2487
	sd888_5g_firmware	2489
	sd888_firmware	2490
	sda429w_firmware	2491
	sda845_firmware	2492
	sdm429w_firmware	2493
	sdm630_firmware	2493
	sdm845_firmware	2494
	sdx12_firmware	2494

Vendor	Product	Page Number
Qualcomm	sdx24_firmware	2494
	sdx50m_firmware	2495
	sdx55m_firmware	2496
	sdx55_firmware	2498
	sdx57m_firmware	2499
	sdx65_firmware	2500
	sdxr1_firmware	2500
	sdxr2_5g_firmware	2501
	sd_455_firmware	2503
	sd_636_firmware	2503
	sd_675_firmware	2504
	sd_8cx_firmware	2505
	sd_8cx_gen2_firmware	2505
	sd_8cx_gen3_firmware	2506
	sd_8_gen1_5g_firmware	2506
	sg4150p_firmware	2508
	sm4125_firmware	2508
	sm4350-ac_firmware	2509
	sm4350_firmware	2510
	sm4375_firmware	2510
	sm4450_firmware	2511
	sm6225-ad_firmware	2511
	sm6225_firmware	2512
	sm6250p_firmware	2512
	sm6250_firmware	2512
	sm6375_firmware	2513
	sm7250p_firmware	2514
	sm7315_firmware	2515
	sm7325p_firmware	2516
	sm8350-ac_firmware	2517
	sm8350_firmware	2517
	sm8450_firmware	2518

Vendor	Product	Page Number
Qualcomm	sm8475_firmware	2518
	smart_audio_100_platform_firmware	2518
	snapdragon_855\+\/860_firmware	2518
	snapdragon_855_firmware	2519
	snapdragon_865\+_5g_firmware	2519
	snapdragon_865_5g_firmware	2520
	snapdragon_870_5g_firmware	2522
	snapdragon_8_gen_1_firmware	2523
	snapdragon_ar2_gen_1_platform_firmware	2524
	snapdragon_auto_4g_modem_firmware	2525
	snapdragon_auto_5g_modem-rf_firmware	2525
	snapdragon_w5\+_gen_1_firmware	2525
	snapdragon_w5\+_gen_1_wearable_platform_firmware	2526
	snapdragon_wear_4100\+_firmware	2526
	snapdragon_wear_4100\+_platform_firmware	2526
	snapdragon_x12_lte_modem_firmware	2526
	snapdragon_x24_lte_modem_firmware	2527
	snapdragon_x50_5g_modem-rf_system_firmware	2527
	snapdragon_x55_5g_firmware	2527
	snapdragon_x55_5g_modem-rf_system_firmware	2529
	snapdragon_x65_5g_modem-rf_system_firmware	2529
	snapdragon_xr1_platform_firmware	2529
	snapdragon_xr2\+_gen_1_platform_firmware	2529
	snapdragon_xr2_5g_firmware	2530
	snapdragon_xr2_5g_platform_firmware	2531
	ssg2115p_firmware	2531
	ssg2125p_firmware	2532
	sw5100p_firmware	2533
	sw5100_firmware	2536

Vendor	Product	Page Number
Qualcomm	sxr1120_firmware	2539
	sxr1230p_firmware	2539
	sxr2130_firmware	2539
	sxr2150p_firmware	2541
	sxr2230p_firmware	2542
	wcd9306_firmware	2542
	wcd9326_firmware	2543
	wcd9330_firmware	2544
	wcd9335_firmware	2544
	wcd9340_firmware	2546
	wcd9341_firmware	2547
	wcd9360_firmware	2550
	wcd9370_firmware	2551
	wcd9371_firmware	2554
	wcd9375_firmware	2555
	wcd9380_firmware	2556
	wcd9385_firmware	2559
	wcn3610_firmware	2561
	wcn3615_firmware	2563
	wcn3620_firmware	2564
	wcn3660b_firmware	2564
	wcn3660_firmware	2567
	wcn3680b_firmware	2568
	wcn3680_firmware	2571
	wcn3910_firmware	2572
	wcn3950_firmware	2573
	wcn3980_firmware	2576
	wcn3988_firmware	2580
	wcn3990_firmware	2583
	wcn3991_firmware	2584
	wcn3998_firmware	2586
	wcn3999_firmware	2588

Vendor	Product	Page Number
Qualcomm	wcn6740_firmware	2589
	wcn6750_firmware	2590
	wcn6850_firmware	2591
	wcn6851_firmware	2593
	wcn6855_firmware	2594
	wcn6856_firmware	2596
	wcn685x-1_firmware	2597
	wcn685x-5_firmware	2597
	wcn7850_firmware	2598
	wcn7851_firmware	2599
	wcn785x-1_firmware	2600
	wcn785x-5_firmware	2600
	wsa8810_firmware	2600
	wsa8815_firmware	2604
	wsa8830_firmware	2607
	wsa8832_firmware	2611
	wsa8835_firmware	2612
Redhat	enterprise_linux	2615
renault	zoe_ev_2021_firmware	2621
Rockwellautomation	armor_powerflex_firmware	2621
ruijie	rg-ew1200g_firmware	2622
Samsung	android	2623
	galaxy_book2_go_firmware	2637
	galaxy_book2_pro_360_firmware	2637
	galaxy_book_go_5g_firmware	2638
	galaxy_book_go_firmware	2638
	s3nrn4v_firmware	2639
	s3nrn82_firmware	2639
	s3nsen4_firmware	2640
	s3nsn4v_firmware	2640
	sen82ab_firmware	2640
shelly	pro_4pm_firmware	2641

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: a2technology					
Product: camera_trap_tracking_system					
Affected Version(s): * Up to (excluding) 3.1905					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in a2 Camera Trap Tracking System allows SQL Injection.This issue affects Camera Trap Tracking System: before 3.1905. **CVE ID : CVE-2023-3386**	N/A	A-A2T-CAME-210823/1
Product: license_portal_system					
Affected Version(s): * Up to (excluding) 1.48					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in a2 License Portal System allows SQL Injection.This issue affects License Portal System: before 1.48. **CVE ID : CVE-2023-3522**	N/A	A-A2T-LICE-210823/2
Vendor: Adiscon					
Product: loganalyzer					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.1.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	A Cross Site Scripting (XSS) vulnerability in Adiscon Aiscon LogAnalyzer through 4.1.13 allows a remote attacker to execute arbitrary code via the asktheoracle.php, details.php, index.php, search.php, export.php, reports.php, and statistics.php components. **CVE ID : CVE-2023-36306**	N/A	A-ADI-LOGA-210823/3
Vendor: Admidio					
Product: admidio					
Affected Version(s): * Up to (excluding) 4.2.11					
Insufficient Session Expiration	06-Aug-2023	6.5	Insufficient Session Expiration in GitHub repository admidio/admidio prior to 4.2.11. **CVE ID : CVE-2023-4190**	https://github.com/admidio/admidio/commit/391fb2af5bee641837a58e7dd66ff76eac92bb74, https://huntr.dev/bounties/71bc75d2-320c-4332-ad11-9de535a06d92	A-ADM-ADMI-210823/4
Vendor: admiror-design-studio					
Product: admiror_gallery					
Affected Version(s): From (including) 5.0.0 Up to (including) 5.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in advcomsys.com oneVote component for Joomla. It allows XSS Targeting Non-Script Elements. **CVE ID : CVE-2023-38045**	N/A	A-ADM-ADMI-210823/5
Vendor: Adobe					
Product: acrobat					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30514.10514					
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38222**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/7
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38223**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/8
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30467 (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-2023-38224**	ts/acrobat/apsb23-30.html	
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38225**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/10
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38226**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/12
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38228**		
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/14
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38233**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/16
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38246**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29303**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/18
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38229**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38230**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/20
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38235**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/22
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38236**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38237**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/24
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30467 (and earlier) are 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-2023-38238**	ts/acrobat/apsb23-30.html	
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38239**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38240**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/27
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38241**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38242**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/29
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/30

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-2023-38243**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/31
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38247**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/33
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38248**		
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 20.001.30005 Up to (including) 20.005.30516.10516					
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/36
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38222		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38223**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/38
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38225**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/40
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/42
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38228**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/44
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/46
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38246**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29303**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/48
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38229**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38230**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/50
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/51

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-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38235**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/52
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38236**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38237**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/54
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38238**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38239**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/56
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38240**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38241**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/58
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38242**	ts/acrobat/apsb23-30.html	
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38243**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/61
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38247**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/63
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38248**		
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/65
Product: acrobat_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 23.003.20269					
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38222**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/67
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38223**	ts/acrobat/apsb23-30.html	
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/69
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38225**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/71
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free vulnerability that could result in	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38227**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38228**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/73
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38231**		
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/75
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38234**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38246**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/77
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/78

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-2023-29303**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38229**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/79
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38230**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38232**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/81
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38235**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38236**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/83
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38237**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38238**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/85
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38239**	ts/acrobat/apsb23-30.html	
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38240**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38241**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/88
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38242**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38243**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/90
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/91

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-2023-38244**		
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/92
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38247**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38248**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/94
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**		
Product: acrobat_reader					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30514.10514					
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-29320**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38222**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/97
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38223		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/99
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38225**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/101
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38228**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/103
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/105
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38246**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/107
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29303		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38229**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/109
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38230**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38232**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/111
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38235**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38236**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/113
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38237**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38238**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/115
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38239**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38240**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/117
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38241**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38242**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/119
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30467 (and earlier) are 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-2023-38243**	ts/acrobat/apsb23-30.html	
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/122
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38247**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38248**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/124
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**		
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30516.10516					
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/126
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38222**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38223**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/128
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38224**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38225**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/130
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38226**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/132
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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/acrobat/apsb23-30.html	A-ADO-ACRO-210823/133

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-2023-38228**		
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/134
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38233**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/136
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38246**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29303**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/138
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/139

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-2023-38229**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38230**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/140
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38235**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/142
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38236**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38237**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/144
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38238**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38239**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/146
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38240**	ts/acrobat/apsb23-30.html	
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38241**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38242**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/149
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38243**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/151
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38247**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/153
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38248**		
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/155
Product: acrobat_reader_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 23.003.20269					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/156
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38222		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38223**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/158
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38225**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/160
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/162
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38228**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/164
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/166
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38246**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29303**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/168
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38229**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38230**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/170
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/171

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-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38235**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/172
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38236**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38237**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/174
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38238**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38239**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/176
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38240**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38241**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/178
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-210823/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38242**	ts/acrobat/apsb23-30.html	
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38243**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/181
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38247**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/183
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38248**		
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	A-ADO-ACRO-210823/185
Product: commerce					
Affected Version(s): * Up to (excluding) 2.4.4					
XML Injection (aka Blind XPath Injection)	09-Aug-2023	7.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and	https://helpx.adobe.com/security/products/magento/a	A-ADO-COMM-210823/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38207**	psb23-42.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38208**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/187
Incorrect Authorization	09-Aug-2023	6.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and	https://helpx.adobe.com/security/products/magento/a	A-ADO-COMM-210823/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38209**	psb23-42.html	
Affected Version(s): 2.4.4					
XML Injection (aka Blind XPath Injection)	09-Aug-2023	7.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38207**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/189
Improper Neutralization of Special Elements used in an	09-Aug-2023	7.2	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38208**		
Incorrect Authorization	09-Aug-2023	6.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38209**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/191
Affected Version(s): 2.4.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	09-Aug-2023	7.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38207**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/192
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38208**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	09-Aug-2023	6.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38209**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/194
Affected Version(s): 2.4.6					
XML Injection (aka Blind XPath Injection)	09-Aug-2023	7.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38207**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38208**	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/196
Incorrect Authorization	09-Aug-2023	6.5	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not	https://helpx.adobe.com/security/products/magento/apsb23-42.html	A-ADO-COMM-210823/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require user interaction. **CVE ID : CVE-2023-38209**		
Product: dimension					
Affected Version(s): * Up to (including) 3.4.9					
Use After Free	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 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-2023-38211**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	A-ADO-DIME-210823/198
Heap-based Buffer Overflow	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 is affected by a Heap-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-2023-38212**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	A-ADO-DIME-210823/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Aug-2023	5.5	Adobe Dimension version 3.4.9 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-2023-38213**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	A-ADO-DIME-210823/200
Product: xmp_toolkit_software_development_kit					
Affected Version(s): * Up to (including) 2022.06					
Uncontrolled Resource Consumption	10-Aug-2023	5.5	Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/xmpcore/apsb23-45.html	A-ADO-XMP_-210823/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38210		
Vendor: Advantech					
Product: webaccess\/scada					
Affected Version(s): * Up to (excluding) 9.1.4					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Aug-2023	9.8	All versions prior to 9.1.4 of Advantech WebAccess/SCADA are vulnerable to use of untrusted pointers. The RPC arguments the client sent client could contain raw memory pointers for the server to use as-is. This could allow an attacker to gain access to the remote file system and the ability to execute commands and overwrite files. **CVE ID : CVE-2023-1437**	N/A	A-ADV-WEBA-210823/202
Vendor: Aerospike					
Product: aerospike_java_client					
Affected Version(s): * Up to (excluding) 4.5.0					
Deserialization of Untrusted Data	04-Aug-2023	9.8	The Aerospike Java client is a Java application that implements a network protocol to communicate with an Aerospike server. Prior to versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 some of the messages received from the server contain Java objects	https://github.com/aerospike/aerospike-client-java/security/advisories/GHSA-jj95-55cr-9597, https://github.com/aerospike/aerospike-client-java/commit/	A-AER-AERO-210823/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that the client deserializes when it encounters them without further validation. Attackers that manage to trick clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. This can be abused to take control of the machine the client is running on. Versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 contain a patch for this issue. **CVE ID : CVE-2023-36480**	80c508cc5ecb0173ce92d7fab8cfab5e77bd9900	
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2.0					
Deserialization of Untrusted Data	04-Aug-2023	9.8	The Aerospike Java client is a Java application that implements a network protocol to communicate with an Aerospike server. Prior to versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 some of the messages received from the server contain Java objects that the client deserializes when it encounters them	https://github.com/aerospike/aerospike-client-java/security/advisories/GHSA-jj95-55cr-9597, https://github.com/aerospike/aerospike-client-java/commit/80c508cc5ecb0173ce92d7fa	A-AER-AERO-210823/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without further validation. Attackers that manage to trick clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. This can be abused to take control of the machine the client is running on. Versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 contain a patch for this issue. **CVE ID : CVE-2023-36480**	b8cfab5e77bd9900	
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.2.0					
Deserialization of Untrusted Data	04-Aug-2023	9.8	The Aerospike Java client is a Java application that implements a network protocol to communicate with an Aerospike server. Prior to versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 some of the messages received from the server contain Java objects that the client deserializes when it encounters them without further validation. Attackers that manage to trick	https://github.com/aerospike/aerospike-client-java/security/advisories/GHSA-jj95-55cr-9597, https://github.com/aerospike/aerospike-client-java/commit/80c508cc5ecb0173ce92d7fab8cfab5e77bd9900	A-AER-AERO-210823/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. This can be abused to take control of the machine the client is running on. Versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 contain a patch for this issue. **CVE ID : CVE-2023-36480**		
Vendor: agentejo					
Product: cockpit					
Affected Version(s): * Up to (excluding) 2.6.3					
Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	06-Aug-2023	8.8	PHP Remote File Inclusion in GitHub repository cockpit-hq/cockpit prior to 2.6.3. **CVE ID : CVE-2023-4195**	https://github.com/cockpit-hq/cockpit/commit/800c05f1984db291769ffa5fdfb1d3e50968e95b, https://huntr.dev/bounties/0bd5da2f-0e29-47ce-90f3-06518656bfd6	A-AGE-COCK-210823/206
Improper Neutralization of Input During	06-Aug-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.6.3.	https://github.com/cockpit-hq/cockpit/commit/039a00cc310bff128c	A-AGE-COCK-210823/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-4196**	a6e6c1c46c6fbad0385c2c, https://huntr.dev/bounties/c275a2d4-721f-49f7-8787-b146af2056a0	
Vendor: agoric					
Product: ses					
Affected Version(s): 0.16.0					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as few as no endowments can gain access to the surrounding host's dynamic import by using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This typically only allows access to module code on the host's file system and is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			threat. That will look like an implementation of `fxFindModule` in a file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Affected Version(s): 0.17.0					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endowments can gain access to the surrounding host's dynamic import by using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows access to module code on the host's file system and is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like an implementation of `fxFindModule` in a file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Affected Version(s): From (including) 0.13.0 Up to (excluding) 0.13.5					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain access to the surrounding host's dynamic import by using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only allows access to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module code on the host's file system and is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look like an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementation of `fxFindModule` in a file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Affected Version(s): From (including) 0.14.0 Up to (excluding) 0.14.5					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can gain access to the	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			surrounding host's dynamic import by using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only allows access to module code on the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			host's file system and is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look like an implementation of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`fxFindModule` in a file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Affected Version(s): From (including) 0.15.0 Up to (excluding) 0.15.24					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can gain access to the surrounding host's	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dynamic import by using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only allows access to module code on the host's file system and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look like an implementation of `fxFindModule` in a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Affected Version(s): From (including) 0.18.0 Up to (excluding) 0.18.7					
N/A	08-Aug-2023	9.8	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can gain access to the surrounding host's dynamic import by	https://github.com/endojs/endo/commit/fc90c6429604dc79ce8e3355e236ccce2bada041, https://github.com/endojs/endo/security/advisories/GHSA-9c4h-3f7h-322r	A-AGO-SES-210823/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using dynamic import after the spread operator, like `{...import(arbitrary ModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only allows access to module code on the host's file system and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look like an implementation of `fxFindModule` in a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file like `xsPlatform.c` that calls `fxRejectModuleFile`. **CVE ID : CVE-2023-39532**		
Vendor: ai-dev					
Product: ai-table					
Affected Version(s): * Up to (excluding) 0.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2023	9.8	ai-dev aitable before v0.2.2 was discovered to contain a SQL injection vulnerability via the component /includes/ajax.php. **CVE ID : CVE-2023-33665**	https://security.friendsofpresta.org/modules/2023/08/01/aitable.html	A-AI--AI-T-210823/214
Product: aioptimizedcombinations					
Affected Version(s): * Up to (excluding) 0.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	9.8	ai-dev aioptimizedcombinations before v0.1.3 was discovered to contain a SQL injection vulnerability via the component /includes/ajax.php. **CVE ID : CVE-2023-33666**	https://security.friendsofpresta.org/modules/2023/08/03/aioptimizedcombinations.html	A-AI--AIOP-210823/215
Vendor: ajaxmanager_project					
Product: ajaxmanager					
Affected Version(s): * Up to (including) 2.3.0					
Unrestricted Upload of File with	01-Aug-2023	9.8	An Unrestricted Upload of File with Dangerous Type vulnerability in the	https://security.friendsofpresta.org/module/2023/07/	A-AJA-AJAX-210823/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Ajaxmanager File and Database explorer (ajaxmanager) module for PrestaShop through 2.3.0, allows remote attackers to upload dangerous files without restrictions. **CVE ID : CVE-2023-33493**	28/ajaxmanager.html	
Vendor: alteryx					
Product: alteryx_server					
Affected Version(s): 2022.1.1.42590					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Alteryx Server 2022.1.1.42590 does not employ file type verification for uploaded files. This vulnerability allows attackers to upload arbitrary files by changing the extension of the uploaded file. **CVE ID : CVE-2023-26961**	http://alteryx.com	A-ALT-ALTE-210823/217
Vendor: AMD					
Product: amd_uprof					
Affected Version(s): * Up to (excluding) 4.1-424					
N/A	08-Aug-2023	7.8	Insufficient validation in the IOCTL (Input Output Control) input buffer in AMD uProf may allow an	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	A-AMD-AMD_-210823/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to load an unsigned driver potentially leading to arbitrary kernel execution. **CVE ID : CVE-2023-20562**		
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary buffer potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20556**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	A-AMD-AMD_-210823/219
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary address potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20561**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	A-AMD-AMD_-210823/220
Affected Version(s): * Up to (excluding) 4.1.396					
N/A	08-Aug-2023	7.8	Insufficient validation in the IOCTL (Input Output Control) input buffer	https://www.amd.com/en/corporate/product-	A-AMD-AMD_-210823/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in AMD uProf may allow an authenticated user to load an unsigned driver potentially leading to arbitrary kernel execution. **CVE ID : CVE-2023-20562**	security/bulletin/AMD-SB-7003	
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary buffer potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20556**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	A-AMD-AMD_-210823/222
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary address potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20561**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	A-AMD-AMD_-210823/223
Vendor: anadnet					
Product: quick_page\/post_redirect_plugin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anadnet Quick Page/Post Redirect Plugin plugin <= 5.2.3 versions. **CVE ID : CVE-2023-25063**	N/A	A-ANA-QUIC-210823/224
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.1.0					
Weak Password Requirements	03-Aug-2023	8.8	Weak Password Requirements in GitHub repository answerdev/answer prior to v1.1.0. **CVE ID : CVE-2023-4125**	https://github.com/answerdev/answer/commit/7d23b17cdbbefcd2e7b5c3150f0b5ec908dc835f, https://huntr.dev/bounties/85bfd18f-8d3b-4154-8b7b-1f8fcf704e28	A-ANS-ANSW-210823/225
Insufficient Session Expiration	03-Aug-2023	8.8	Insufficient Session Expiration in GitHub repository answerdev/answer prior to v1.1.0. **CVE ID : CVE-2023-4126**	https://huntr.dev/bounties/7f50bf1c-bcb9-46ca-8cec-211493d280c5, https://github.com/answerdev/answer/commit/4f468b58d0dea51290bfbdd3e963	A-ANS-ANSW-210823/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				32b0014c8730	
Affected Version(s): * Up to (excluding) 1.1.1					
Missing Authorization	03-Aug-2023	6.5	Missing Authorization in GitHub repository answerdev/answer prior to v1.1.1. **CVE ID : CVE-2023-4124**	https://huntr.dev/bounties/2c684f99-d181-4106-8ee2-64a76ae6a348, https://github.com/answerdev/answer/commit/964195fd859ee5d7171fac847374dfa31893e793	A-ANS-ANSW-210823/227
Race Condition within a Thread	03-Aug-2023	5.9	Race Condition within a Thread in GitHub repository answerdev/answer prior to v1.1.1. **CVE ID : CVE-2023-4127**	https://github.com/answerdev/answer/commit/47661dc8a356ce6aa7793f1bd950399292180182, https://huntr.dev/bounties/cf7d19e3-1318-4c77-8366-d8d04a0b41ba	A-ANS-ANSW-210823/228
Vendor: anujkumar					
Product: maid_hiring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	08-Aug-2023	4.8	Maid Hiring Management System v1.0 was discovered to contain a SQL injection	N/A	A-ANU-MAID-210823/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability in the Admin page. **CVE ID : CVE-2023-37688**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Maid Hiring Management System v1.0 was discovered to contain a SQL injection vulnerability in the Booking Request page. **CVE ID : CVE-2023-37689**	N/A	A-ANU-MAID-210823/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Maid Hiring Management System v1.0 was discovered to contain a SQL injection vulnerability in the Search Maid page. **CVE ID : CVE-2023-37690**	N/A	A-ANU-MAID-210823/231
Product: online_nurse_hiring_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.2	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the View Request of Nurse Page in the Admin portal. **CVE ID : CVE-2023-37687**	N/A	A-ANU-ONLI-210823/232
Improper Neutralization of Input During	08-Aug-2023	4.8	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS)	N/A	A-ANU-ONLI-210823/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			vulnerability in the Profile Page of the Admin. **CVE ID : CVE-2023-37683**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Search Report Details of the Admin portal. **CVE ID : CVE-2023-37684**	N/A	A-ANU-ONLI-210823/234
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Search Report Page of the Admin portal. **CVE ID : CVE-2023-37685**	N/A	A-ANU-ONLI-210823/235
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Add Nurse Page in the Admin portal. **CVE ID : CVE-2023-37686**	N/A	A-ANU-ONLI-210823/236
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Aug-2023	8.8	Execution with Unnecessary Privileges, : Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Airflow.The "Run Task" feature enables authenticated user to bypass some of the restrictions put in place. It allows to execute code in the webserver context as well as allows to bypas limitation of access the user has to certain DAGs. The "Run Task" feature is considered dangerous and it has been removed entirely in Airflow 2.6.0 This issue affects Apache Airflow: before 2.6.0. **CVE ID : CVE-2023-39508**	https://github.com/apache/airflow/pull/29706, https://lists.apache.org/thread/j2nkjd0zqvtqk85s6ywpx3c35pvzyx15	A-APA-AIRF-210823/237
Product: roller					
Affected Version(s): * Up to (excluding) 6.1.2					
Improper Neutralization of Input During Web Page	06-Aug-2023	5.4	Insufficient input validation and sanitation in Weblog Category name, Website About and File Upload features	https://lists.apache.org/thread/n9mjhhlm7z7b7to646tkvf3otkf21flp	A-APA-ROLL-210823/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			in all versions of Apache Roller on all platforms allows an authenticated user to perform an XSS attack. Mitigation: if you do not have Roller configured for untrusted users, then you need to do nothing because you trust your users to author raw HTML and other web content. If you are running with untrusted users then you should upgrade to Roller 6.1.2 and you should disable Roller's File Upload feature.? **CVE ID : CVE-2023-37581**		
Product: traffic_server					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.1.7					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	09-Aug-2023	9.1	Improper Input Validation vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1. **CVE ID : CVE-2023-33934**	https://lists.apache.org/thread/jsl6dfdgs1mjjo1mbtyflyjr7xftswhc	A-APA-TRAF-210823/239
Affected Version(s): From (including) 9.0.0 Up to (including) 9.2.1					
Inconsistent Interpretation of	09-Aug-2023	9.1	Improper Input Validation vulnerability in Apache Software	https://lists.apache.org/thread/jsl6dfdgs	A-APA-TRAF-210823/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
HTTP Requests ('HTTP Request Smuggling')			Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1. **CVE ID : CVE-2023-33934**	1mjjo1mbtyflyjr7xftswhc	
Vendor: Artifex					
Product: ghostscript					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Aug-2023	5.5	A buffer overflow flaw was found in base/gdevdevn.c:1973 in devn_pcx_write_rle() in ghostscript. This issue may allow a local attacker to cause a denial of service via outputting a crafted PDF file for a DEVN device with gs. **CVE ID : CVE-2023-38559**	https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=d81b82c70bc1	A-ART-GHOS-210823/241
Integer Overflow or Wraparound	01-Aug-2023	5.5	An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format. **CVE ID : CVE-2023-38560**	https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=b7eb1d0174c	A-ART-GHOS-210823/242
Vendor: assaabloy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: control_id_idsecure					
Affected Version(s): * Up to (including) 4.7.26.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2023	9.8	A SQL injection vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing unauthenticated attackers to write PHP files on the server's root directory, resulting in remote code execution. **CVE ID : CVE-2023-33367**	N/A	A-ASS-CONT-210823/243
Use of Hard-coded Credentials	03-Aug-2023	9.8	Control ID IDSecure 4.7.26.0 and prior uses a hardcoded cryptographic key in order to sign and verify JWT session tokens, allowing attackers to sign arbitrary session tokens and bypass authentication. **CVE ID : CVE-2023-33371**	https://www.controlid.com.br/en/access-control/idsecure/	A-ASS-CONT-210823/244
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	9.1	A path traversal vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing attackers to delete arbitrary files on IDSecure filesystem, causing a denial of service. **CVE ID : CVE-2023-33369**	https://www.controlid.com.br/en/access-control/idsecure/	A-ASS-CONT-210823/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	03-Aug-2023	7.5	An uncaught exception vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing attackers to cause the main web server of IDSecure to fault and crash, causing a denial of service. **CVE ID : CVE-2023-33370**	https://www.controlid.com.br/en/access-control/idsecure/	A-ASS-CONT-210823/246
Exposure of Resource to Wrong Sphere	03-Aug-2023	6.5	Some API routes exists in Control ID IDSecure 4.7.26.0 and prior, exfiltrating sensitive information and passwords to users accessing these API routes. **CVE ID : CVE-2023-33368**	https://www.controlid.com.br/en/access-control/idsecure/	A-ASS-CONT-210823/247
Vendor: Axis					
Product: license_plate_verifier					
Affected Version(s): * Up to (including) 2.8.3					
Improper Handling of Exceptional Conditions	03-Aug-2023	9.8	Due to insufficient file permissions, unprivileged users could gain access to unencrypted user credentials that are used in the integration interface towards 3rd party systems. **CVE ID : CVE-2023-21408**	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	03-Aug-2023	9.8	Due to insufficient file permissions, unprivileged users could gain access to unencrypted administrator credentials allowing the configuration of the application. **CVE ID : CVE-2023-21409**	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/249
N/A	03-Aug-2023	8.8	A broken access control was found allowing for privileged escalation of the operator account to gain administrator privileges. **CVE ID : CVE-2023-21407**	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/250
N/A	03-Aug-2023	8.8	User provided input is not sanitized on the AXIS License Plate Verifier specific “api.cgi” allowing for arbitrary code execution. **CVE ID : CVE-2023-21410**	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/251
N/A	03-Aug-2023	8.8	User provided input is not sanitized in the “Settings > Access Control” configuration interface allowing for arbitrary code execution.	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21411		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	8.8	User provided input is not sanitized on the AXIS License Plate Verifier specific "search.cgi" allowing for SQL injections. **CVE ID : CVE-2023-21412**	https://www.axis.com/dam/public/0b/1c/96/cve-2023-2140712-en-US-409778.pdf	A-AXI-LICE-210823/253
Vendor: bestaddon					
Product: bestaddon_gallery					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection. **CVE ID : CVE-2023-23757**	N/A	A-BES-BEST-210823/254
Vendor: bitberry					
Product: file_opener					
Affected Version(s): 23.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Aug-2023	7.8	An issue in the CAB file extraction function of Bitberry File Opener v23.0 allows attackers to execute a directory traversal. **CVE ID : CVE-2023-37646**	N/A	A-BIT-FILE-210823/255
Vendor: bkmacdaddy					
Product: pinterest_rss_widget					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in bkmacdaddy designs Pinterest RSS Widget plugin <= 2.3.1 versions. **CVE ID : CVE-2023-23877**	N/A	A-BKM-PINT-210823/256
Vendor: bluetens					
Product: bluetensq					
Affected Version(s): 4.3.15					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-Aug-2023	3.1	Bluetens Electrostimulation Device BluetensQ device app version 4.3.15 is vulnerable to Man-in-the-middle attacks in the BLE channel. It allows attackers to decrease or increase the intensity of the stimulator by hijacking the BLE communication. **CVE ID : CVE-2023-26979**	N/A	A-BLU-BLUE-210823/257
Vendor: braincert					
Product: virtual_classroom					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.25.0					
Improper Neutralization of Special Elements used in an SQL	07-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	N/A	A-BRA-VIRT-210823/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			vulnerability allows SQL Injection. **CVE ID : CVE-2023-34477**		
Vendor: brandid					
Product: social_proof_\(testimonial\)_slider					
Affected Version(s): * Up to (including) 2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in brandiD Social Proof (Testimonial) Slider plugin <= 2.2.3 versions. **CVE ID : CVE-2023-24389**	N/A	A-BRA-SOCI-210823/259
Vendor: byzoro					
Product: smart_s85f					
Affected Version(s): * Up to (including) 20230722					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20230722 and classified as critical. This issue affects some unknown processing of the file importhtml.php. The manipulation of the argument sql leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier	N/A	A-BYZ-SMAR-210823/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-235967. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4120**		
Unrestricted Upload of File with Dangerous Type	03-Aug-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20230722. It has been classified as critical. Affected is an unknown function. The manipulation of the argument file_upload leads to unrestricted upload. 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-235968. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4121**	N/A	A-BYZ-SMAR-210823/261
Vendor: cartflows					
Product: cartflows					
Affected Version(s): * Up to (including) 1.11.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CartFlows Pro plugin <= 1.11.11 versions. **CVE ID : CVE-2023-36686**	N/A	A-CAR-CART-210823/262
Vendor: cdwanjiang					
Product: flash_flood_disaster_monitoring_and_warning_system					
Affected Version(s): 2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2023	7.5	A vulnerability, which was classified as problematic, has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This issue affects some unknown processing of the file \Service\FileHandler.ashx. The manipulation of the argument FileDirectory leads to absolute path traversal. 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-236207. **CVE ID : CVE-2023-4172**	N/A	A-CDW-FLAS-210823/263
Path Traversal: '../filedir'	05-Aug-2023	5.3	A vulnerability classified as problematic was	N/A	A-CDW-FLAS-210823/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This vulnerability affects unknown code of the file \Service\FileDownload.ashx. The manipulation of the argument Files leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-236206 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-4171**		
Vendor: Chamilo					
Product: chamilo					
Affected Version(s): From (including) 1.11.0 Up to (including) 1.11.18					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	9.8	A command injection vulnerability in the wsConvertPpt component of Chamilo v1.11.* up to v1.11.18 allows attackers to execute arbitrary commands via a SOAP API call with a crafted PowerPoint name. **CVE ID : CVE-2023-34960**	https://support.chamilo.org/projects/1/wiki/Security_issues#Issue-112-2023-04-20-Critical-impact-High-risk-Remote-Code-Execution	A-CHA-CHAM-210823/265
Vendor: churchcrm					
Product: churchcrm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the role and gender parameters within the /QueryView.php component. **CVE ID : CVE-2023-38760**	N/A	A-CHU-CHUR-210823/266
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the friendmonths parameter within the /QueryView.php. **CVE ID : CVE-2023-38762**	N/A	A-CHU-CHUR-210823/267
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the birthmonth and percls parameters within the /QueryView.php. **CVE ID : CVE-2023-38764**	N/A	A-CHU-CHUR-210823/268
Improper Neutralization of Special Elements	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain	N/A	A-CHU-CHUR-210823/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			sensitive information via the membermonth parameter within the /QueryView.php. **CVE ID : CVE-2023-38765**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the 'value' and 'custom' parameters within the /QueryView.php. **CVE ID : CVE-2023-38767**	N/A	A-CHU-CHUR-210823/270
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the PropertyID parameter within the /QueryView.php. **CVE ID : CVE-2023-38768**	N/A	A-CHU-CHUR-210823/271
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the searchstring and searchwhat parameters within the /QueryView.php.	N/A	A-CHU-CHUR-210823/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38769		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the group parameter within the /QueryView.php. **CVE ID : CVE-2023-38770**	N/A	A-CHU-CHUR-210823/273
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the volopp parameter within the /QueryView.php. **CVE ID : CVE-2023-38771**	N/A	A-CHU-CHUR-210823/274
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the volopp1 and volopp2 parameters within the /QueryView.php. **CVE ID : CVE-2023-38773**	N/A	A-CHU-CHUR-210823/275
Improper Neutralization of Special Elements used in an	08-Aug-2023	6.5	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information	N/A	A-CHU-CHUR-210823/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			via the FundRaiserID parameter within the /FundRaiserEditor.php endpoint. **CVE ID : CVE-2023-38763**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Cross Site Scripting (XSS) vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to execute arbitrary code via a crafted payload to the systemSettings.php component. **CVE ID : CVE-2023-38761**	N/A	A-CHU-CHUR-210823/277
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Cross Site Scripting (XSS) vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to execute arbitrary code via a crafted payload to the PersonView.php component. **CVE ID : CVE-2023-38766**	N/A	A-CHU-CHUR-210823/278
Vendor: Cisco					
Product: broadworks_application_delivery_platform					
Affected Version(s): * Up to (excluding) ri.2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): * Up to (excluding) ri.2023.06					
Improper Neutralization of Input During	03-Aug-2023	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	A-CIS-BROA-210823/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			CommPilot Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20204**	Advisory/cisco-sa-commpilot-xss-jC46sezF	
Product: broadworks_application_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): * Up to (excluding) 2023.06					
Improper Neutralization of Input During	03-Aug-2023	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	A-CIS-BROA-210823/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			CommPilot Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20204**	Advisory/cisco-sa-commpilot-xss-jC46sezF	
Affected Version(s): * Up to (excluding) 23.0.2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): * Up to (excluding) 23.0.2023.08					
Improper Neutralization of Input During Web Page	03-Aug-2023	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-BROA-210823/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20204**	o-sa-commpilot-xss-jC46sezF	
Affected Version(s): From (including) 24.0 Up to (excluding) 24.0.2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): From (including) 24.0 Up to (excluding) 24.0.2023.08					
Improper Neutralization of Input During Web Page	03-Aug-2023	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-BROA-210823/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20204**	o-sa-commpilot-xss-jC46sezF	
Product: broadworks_database_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_execution_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	A-CIS-BROA-210823/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**	Advisory/cisco-sa-bw-priv-esc-qTgUZOsQ	
Product: broadworks_media_server					
Affected Version(s): * Up to (excluding) 2023.05					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20216		
Product: broadworks_network_database_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_network_function_manager					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_network_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): * Up to (excluding) 23.0.2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_profile_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Affected Version(s): * Up to (excluding) 23.0.2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_service_control_function_server					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_troubleshooting_server					
Affected Version(s): * Up to (excluding) 2023.06					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-priv-esc-qTgUZOsQ	A-CIS-BROA-210823/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**		
Product: broadworks_xtended_services_platform					
Affected Version(s): * Up to (excluding) 2023.05					
Incorrect Permission Assignment for Critical Resource	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-BROA-210823/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**	o-sa-bw-priv-esc-qTgUZOsQ	
Affected Version(s): * Up to (excluding) 23.0.2023.05					
Incorrect Permission Assignment for	03-Aug-2023	7.8	A vulnerability in the privilege management functionality of all	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-BROA-210823/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability. **CVE ID : CVE-2023-20216**	/CiscoSecurity Advisory/cisco-sa-bw-priv-esc-qTgUZOsQ	
Affected Version(s): * Up to (excluding) 23.0.2023.08					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20204**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-commpilot-xss-jC46sezF	A-CIS-BROA-210823/300
Product: sd-wan_vmanage					
Affected Version(s): 20.6.3.3					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication	https://sec.cloudapps.cisco.com/security/c	A-CIS-SD-W-210823/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI. **CVE ID : CVE-2023-20214**	enter/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 20.10 Up to (excluding) 20.10.1.2					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	A-CIS-SD-W-210823/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface or the CLI. **CVE ID : CVE-2023-20214**		
Affected Version(s): From (including) 20.11 Up to (excluding) 20.11.1.2					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	A-CIS-SD-W-210823/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI. **CVE ID : CVE-2023-20214**		
Affected Version(s): From (including) 20.6.4 Up to (excluding) 20.6.4.2					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	A-CIS-SD-W-210823/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI. **CVE ID : CVE-2023-20214**		
Affected Version(s): From (including) 20.6.5 Up to (excluding) 20.6.5.5					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	A-CIS-SD-W-210823/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI. **CVE ID : CVE-2023-20214**		
Affected Version(s): From (including) 20.7 Up to (excluding) 20.9.3.2					
Improper Authentication	03-Aug-2023	9.1	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA	A-CIS-SD-W-210823/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI. **CVE ID : CVE-2023-20214**		
Vendor: cloudflare					
Product: odoh-rs					
Affected Version(s): * Up to (excluding) 1.0.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	5.9	A vulnerability was discovered in the odoh-rs rust crate that stems from faulty logic during the parsing of encrypted queries. This issue specifically occurs when processing encrypted query data received from remote clients and enables an attacker with knowledge of this vulnerability to craft and send specially designed encrypted	https://github.com/cloudflare/odoh-rs/pull/28, https://github.com/cloudflare/odoh-rs/security/advisories/GHSA-gpcv-p28p-fv2p	A-CLO-ODOH-210823/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queries to targeted ODOH servers running with odoh-rs. Upon successful exploitation, the server will crash abruptly, disrupting its normal operation and rendering the service temporarily unavailable. **CVE ID : CVE-2023-3766**		
Product: warp					
Affected Version(s): * Up to (excluding) 2023.7.160.0					
Cleartext Transmission of Sensitive Information	03-Aug-2023	6.8	The Cloudflare WARP client for Windows assigns loopback IPv4 addresses for the DNS Servers, since WARP acts as local DNS server that performs DNS queries in a secure manner, however, if a user is connected to WARP over an IPv6-capable network, te WARP client did not assign loopback IPv6 addresses but Unique Local Addresses, which under certain conditions could point towards unknown devices in the same local network which enables an Attacker	https://github.com/cloudflare/advisories/security/advisories/GHSA-mv6g-7577-vq4w	A-CLO-WARP-210823/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to view DNS queries made by the device. **CVE ID : CVE-2023-2754**		
Product: wrangler					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	5.7	The Wrangler command line tool (<=wrangler@3.1.0) was affected by a directory traversal vulnerability when running a local development server for Pages (wrangler pages dev command). This vulnerability enabled an attacker in the same network as the victim to connect to the local development server and access the victim's files present outside of the directory for the development server. **CVE ID : CVE-2023-3348**	https://github.com/cloudflare/workers-sdk/security/advisories/GHSA-8c93-4hch-xgxp	A-CLO-WRAN-210823/309
Vendor: Clusterlabs					
Product: libqb					
Affected Version(s): * Up to (excluding) 2.0.8					
Buffer Copy without Checking Size of Input ('Classic	08-Aug-2023	9.8	log_blackbox.c in libqb before 2.0.8 allows a buffer overflow via long log messages because the header size is not considered.	https://github.com/ClusterLabs/libqb/pull/490, https://github.com/ClusterLabs/libqb/commit/1bbaa9	A-CLU-LIBQ-210823/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2023-39976**	29b77113532785c408dd1b41cd0521ffc8	
Vendor: cmscommander					
Product: wp_shopping_pages					
Affected Version(s): * Up to (including) 1.14					
Cross-Site Request Forgery (CSRF)	07-Aug-2023	6.8	The WP Shopping Pages WordPress plugin through 1.14 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack. **CVE ID : CVE-2023-3492**	N/A	A-CMS-WP_S-210823/311
Vendor: codebard					
Product: codebard\'s_patron_button_and_widgets_for_patreon					
Affected Version(s): * Up to (including) 2.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CodeBard CodeBard's Patron Button and Widgets for Patreon plugin <= 2.1.8 versions. **CVE ID : CVE-2023-30491**	N/A	A-COD-CODE-210823/312
Vendor: Codesys					
Product: control_for_beaglebone_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/315
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/318
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/320
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/323
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/325
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/327
Product: control_for_empc-a\/imx6_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/330
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/333
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/335
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/338
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/340
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/342
Product: control_for_iot2000_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/345
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/348
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/350
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/353
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/355
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/357
Product: control_for_linux_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/360
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/363
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/365
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/368
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/370
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/372
Product: control_for_pfc100_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/375
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/378
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/380
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/383
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/385
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/387
Product: control_for_pfc200_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/390
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/393
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/395
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after	N/A	A-COD-CONT-210823/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/398
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/400
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/402
Product: control_for_plcnext_sl					
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-CONT-210823/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/405
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/408
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via	N/A	A-COD-CONT-210823/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**	N/A	A-COD-CONT-210823/411
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to	N/A	A-COD-CONT-210823/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/413
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a	N/A	A-COD-CONT-210823/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/415
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions,	N/A	A-COD-CONT-210823/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/417
Product: control_for_raspberry_pi_sl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-CONT-210823/418
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-	N/A	A-COD-CONT-210823/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/420
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network	N/A	A-COD-CONT-210823/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550	N/A	A-COD-CONT-210823/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37549		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/423
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the	N/A	A-COD-CONT-210823/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**	N/A	A-COD-CONT-210823/426
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to	N/A	A-COD-CONT-210823/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/428
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a	N/A	A-COD-CONT-210823/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/430
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions,	N/A	A-COD-CONT-210823/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/432
Product: control_for_wago_touch_panels_600_sl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.10.0.0					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-CONT-210823/433
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-	N/A	A-COD-CONT-210823/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**	N/A	A-COD-CONT-210823/436
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially	N/A	A-COD-CONT-210823/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**	N/A	A-COD-CONT-210823/439
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read	N/A	A-COD-CONT-210823/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556.	N/A	A-COD-CONT-210823/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37553		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**	N/A	A-COD-CONT-210823/442
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content	N/A	A-COD-CONT-210823/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-	N/A	A-COD-CONT-210823/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/445
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is	N/A	A-COD-CONT-210823/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/447
Product: control_rte_sl					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally	N/A	A-COD-CONT-210823/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**	N/A	A-COD-CONT-210823/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/450
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.	N/A	A-COD-CONT-210823/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/452
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**		
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be	N/A	A-COD-CONT-210823/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/455
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-	N/A	A-COD-CONT-210823/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/458
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a	N/A	A-COD-CONT-210823/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/460
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions,	N/A	A-COD-CONT-210823/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: control_rte_sl_\(for_beckhoff_cx\)					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-CONT-210823/463
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component	N/A	A-COD-CONT-210823/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**	N/A	A-COD-CONT-210823/466
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.	N/A	A-COD-CONT-210823/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/468
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication	N/A	A-COD-CONT-210823/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-	N/A	A-COD-CONT-210823/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**	N/A	A-COD-CONT-210823/471
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful	N/A	A-COD-CONT-210823/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This	N/A	A-COD-CONT-210823/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**	N/A	A-COD-CONT-210823/474
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication	N/A	A-COD-CONT-210823/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**	N/A	A-COD-CONT-210823/476
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-CONT-210823/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**		
Product: control_runtime_system_toolkit					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-CONT-210823/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**	N/A	A-COD-CONT-210823/479
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially	N/A	A-COD-CONT-210823/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**	N/A	A-COD-CONT-210823/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**	N/A	A-COD-CONT-210823/482
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially	N/A	A-COD-CONT-210823/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**		
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**	N/A	A-COD-CONT-210823/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-CONT-210823/485
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address,	N/A	A-COD-CONT-210823/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556.	N/A	A-COD-CONT-210823/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37554		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-CONT-210823/488
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-CONT-210823/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-CONT-210823/490
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-CONT-210823/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-CONT-210823/492
Product: control_win_sl					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-CONT-210823/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.	N/A	A-COD-CONT-210823/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-CONT-210823/495
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication	N/A	A-COD-CONT-210823/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550	N/A	A-COD-CONT-210823/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37549		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-CONT-210823/498
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In	N/A	A-COD-CONT-210823/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556.	N/A	A-COD-CONT-210823/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37552		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**	N/A	A-COD-CONT-210823/501
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read	N/A	A-COD-CONT-210823/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556.	N/A	A-COD-CONT-210823/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37555		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**	N/A	A-COD-CONT-210823/504
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to	N/A	A-COD-CONT-210823/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**	N/A	A-COD-CONT-210823/506
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an	N/A	A-COD-CONT-210823/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**		
Product: development_system					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-DEVE-210823/508
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-DEVE-210823/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.	N/A	A-COD-DEVE-210823/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**	N/A	A-COD-DEVE-210823/511
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple	N/A	A-COD-DEVE-210823/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.	N/A	A-COD-DEVE-210823/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**		
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**	N/A	A-COD-DEVE-210823/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**	N/A	A-COD-DEVE-210823/515
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an	N/A	A-COD-DEVE-210823/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556.	N/A	A-COD-DEVE-210823/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37554		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**	N/A	A-COD-DEVE-210823/518
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-DEVE-210823/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-DEVE-210823/520
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication	N/A	A-COD-DEVE-210823/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-DEVE-210823/522
Improper Restriction of Excessive Authentica	03-Aug-2023	3.3	A missing Brute-Force protection in CODESYS Development System prior to 3.5.19.20	N/A	A-COD-DEVE-210823/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			allows a local attacker to have unlimited attempts of guessing the password within an import dialog. **CVE ID : CVE-2023-3669**		
Affected Version(s): From (including) 3.5.11.20 Up to (excluding) 3.5.19.20					
Insufficient Verification of Data Authenticity	03-Aug-2023	8.8	In CODESYS Development System versions from 3.5.11.20 and before 3.5.19.20 a missing integrity check might allow an unauthenticated remote attacker to manipulate the content of notifications received via HTTP by the CODESYS notification server. **CVE ID : CVE-2023-3663**	N/A	A-COD-DEVE-210823/524
Affected Version(s): From (including) 3.5.17.0 Up to (excluding) 3.5.19.20					
Uncontrolled Search Path Element	03-Aug-2023	7.3	In CODESYS Development System versions from 3.5.17.0 and prior to 3.5.19.20 a vulnerability allows for execution of binaries from the current working directory in the users context . **CVE ID : CVE-2023-3662**	N/A	A-COD-DEVE-210823/525
Product: hmi					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**	N/A	A-COD-HMI-210823/526
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally	N/A	A-COD-HMI-210823/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37546**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550	N/A	A-COD-HMI-210823/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37547		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**	N/A	A-COD-HMI-210823/529
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component	N/A	A-COD-HMI-210823/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550 **CVE ID : CVE-2023-37549**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549.	N/A	A-COD-HMI-210823/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37550		
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**	N/A	A-COD-HMI-210823/532
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-HMI-210823/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37552**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555	N/A	A-COD-HMI-210823/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CVE-2023-37556. **CVE ID : CVE-2023-37553**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**	N/A	A-COD-HMI-210823/535
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted	N/A	A-COD-HMI-210823/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-HMI-210823/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**		
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**	N/A	A-COD-HMI-210823/538
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service	N/A	A-COD-HMI-210823/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**	N/A	A-COD-HMI-210823/540
Product: safety_sil2					
Affected Version(s): * Up to (excluding) 3.5.19.20					
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-SAFE-210823/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550 **CVE ID : CVE-2023-37545**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550	N/A	A-COD-SAFE-210823/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37546		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37547**	N/A	A-COD-SAFE-210823/543
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the	N/A	A-COD-SAFE-210823/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550 **CVE ID : CVE-2023-37548**		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550	N/A	A-COD-SAFE-210823/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37549		
N/A	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549. **CVE ID : CVE-2023-37550**	N/A	A-COD-SAFE-210823/546
Files or Directories Accessible to External Parties	03-Aug-2023	6.5	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to	N/A	A-COD-SAFE-210823/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller. **CVE ID : CVE-2023-37551**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555	N/A	A-COD-SAFE-210823/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CVE-2023-37556. **CVE ID : CVE-2023-37552**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37553**	N/A	A-COD-SAFE-210823/549
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted	N/A	A-COD-SAFE-210823/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556. **CVE ID : CVE-2023-37554**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-	N/A	A-COD-SAFE-210823/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556. **CVE ID : CVE-2023-37555**		
N/A	03-Aug-2023	6.5	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555. **CVE ID : CVE-2023-37556**	N/A	A-COD-SAFE-210823/552
Out-of-bounds Write	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in	N/A	A-COD-SAFE-210823/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition. **CVE ID : CVE-2023-37557**		
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559 **CVE ID : CVE-2023-37558**	N/A	A-COD-SAFE-210823/554
N/A	03-Aug-2023	6.5	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network	N/A	A-COD-SAFE-210823/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558 **CVE ID : CVE-2023-37559**		
Vendor: connectedio					
Product: connected_io					
Affected Version(s): * Up to (including) 2.1.0					
Use of Hard-coded Credentials	04-Aug-2023	9.8	Connected IO v2.1.0 and prior uses a hard-coded username/password pair embedded in their device's firmware used for device communication using MQTT. An attacker who gained access to these credentials is able to connect to the MQTT broker and send messages on behalf of devices, impersonating them. in order to sign and verify JWT session tokens, allowing attackers to sign arbitrary session	N/A	A-CON-CONN-210823/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tokens and bypass authentication. **CVE ID : CVE-2023-33372**		
Cleartext Storage of Sensitive Information	04-Aug-2023	9.8	Connected IO v2.1.0 and prior keeps passwords and credentials in clear-text format, allowing attackers to exfiltrate the credentials and use them to impersonate the devices. **CVE ID : CVE-2023-33373**	N/A	A-CON-CONN-210823/557
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has a command as part of its communication protocol allowing the management platform to specify arbitrary OS commands for devices to execute. Attackers abusing this dangerous functionality may issue all devices OS commands to execute, resulting in arbitrary remote command execution. **CVE ID : CVE-2023-33374**	N/A	A-CON-CONN-210823/558
Out-of-bounds Write	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has a stack-based buffer overflow vulnerability in its communication	N/A	A-CON-CONN-210823/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol, enabling attackers to take control over devices. **CVE ID : CVE-2023-33375**		
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has an argument injection vulnerability in its iptables command message in its communication protocol, enabling attackers to execute arbitrary OS commands on devices. **CVE ID : CVE-2023-33376**	N/A	A-CON-CONN-210823/560
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has an OS command injection vulnerability in the set firewall command in part of its communication protocol, enabling attackers to execute arbitrary OS commands on devices. **CVE ID : CVE-2023-33377**	N/A	A-CON-CONN-210823/561
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has an argument injection vulnerability in its AT command message in its communication protocol, enabling attackers to execute	N/A	A-CON-CONN-210823/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS commands on devices. **CVE ID : CVE-2023-33378**		
Vendor: Craftercms					
Product: craftercms					
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from 4.0.0 through 4.0.2, from 3.1.0 through 3.1.27. **CVE ID : CVE-2023-4136**	N/A	A-CRA-CRAF-210823/563
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from	N/A	A-CRA-CRAF-210823/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.0.0 through 4.0.2, from 3.1.0 through 3.1.27. **CVE ID : CVE-2023-4136**		
Vendor: Creative-solutions					
Product: contact_form_generator					
Affected Version(s): * Up to (including) 2.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Creative Solutions Contact Form Generator plugin <= 2.5.5 versions. **CVE ID : CVE-2023-37988**	N/A	A-CRE-CONT-210823/565
Product: creative_gallery					
Affected Version(s): From (including) 1.0.0 Up to (including) 2.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection. **CVE ID : CVE-2023-23758**	N/A	A-CRE-CREA-210823/566
Vendor: creativeitem					
Product: academy_learning_management_system					
Affected Version(s): 6.0					
Improper Neutralization of Input During Web Page	04-Aug-2023	6.1	Creative Item Academy LMS 6.0 was discovered to contain a cross-site	N/A	A-CRE-ACAD-210823/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			scripting (XSS) vulnerability. **CVE ID : CVE-2023-38964**		
Product: academy_lms					
Affected Version(s): 6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability has been found in Academy LMS 6.0 and classified as problematic. This vulnerability affects unknown code of the file /academy/home/courses. The manipulation of the argument query/sort_by leads to cross site scripting. The attack can be initiated remotely. VDB-235966 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4119**	N/A	A-CRE-ACAD-210823/568
Vendor: cryptomator					
Product: cryptomator					
Affected Version(s): * Up to (excluding) 1.9.3					
Improper Privilege Management	07-Aug-2023	7.8	Cryptomator encrypts data being stored on cloud infrastructure. The MSI installer	https://github.com/cryptomator/cryptomator/security/advisories/GH	A-CRY-CRYP-210823/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided on the homepage for Cryptomator version 1.9.2 allows local privilege escalation for low privileged users, via the `repair` function. The problem occurs as the repair function of the MSI is spawning an SYSTEM Powershell without the `-NoProfile` parameter. Therefore the profile of the user starting the repair will be loaded. Version 1.9.3 contains a fix for this issue. Adding a `-NoProfile` to the powershell is a possible workaround. **CVE ID : CVE-2023-39520**	SA-62gx-54j7-mjh3, https://github.com/cryptomator/cryptomator/commit/727c32ad50c3901a6144a11cf984a3b7ebcf8b2b	
Vendor: cskaza					
Product: cszcms					
Affected Version(s): 1.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2023	9.8	A SQL injection vulnerability in CSZCMS 1.3.0 allows remote attackers to run arbitrary SQL commands via p parameter or the search URL. **CVE ID : CVE-2023-34545**	N/A	A-CSK-CSZC-210823/570
Vendor: cubiclesoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: barebones_cms					
Affected Version(s): 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	5.4	The Barebones CMS v2.0.2 is vulnerable to Stored Cross-Site Scripting (XSS) when an authenticated user interacts with certain features on the admin panel. **CVE ID : CVE-2023-36211**	N/A	A-CUB-BARE-210823/571
Vendor: dango					
Product: dango-translator					
Affected Version(s): 4.5.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2023	9.8	Dango-Translator v4.5.5 was discovered to contain a remote command execution (RCE) vulnerability via the component app/config/cloud_config.json. **CVE ID : CVE-2023-38942**	https://github.com/PantsuDango/Dango-Translator/issues/127	A-DAN-DANG-210823/572
Vendor: datadoghq					
Product: import-in-the-middle					
Affected Version(s): * Up to (excluding) 1.4.2					
N/A	07-Aug-2023	9.8	import-in-the-middle is a module loading interceptor specifically for ESM modules. The import-in-the-middle loader works by generating a wrapper module on the fly. The wrapper uses the module	https://github.com/DataDog/import-in-the-middle/commit/2531cdd9d1d73f9eaa87c16967f60cb276c1971b	A-DAT-IMPO-210823/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifier to load the original module and add some wrapping code. Prior to version 1.4.2, it allows for remote code execution in cases where an application passes user-supplied input directly to the `import()` function. This vulnerability has been patched in import-in-the-middle version 1.4.2. Some workarounds are available. Do not pass any user-supplied input to `import()`. Instead, verify it against a set of allowed values. If using import-in-the-middle, directly or indirectly, and support for EcmaScript Modules is not needed, ensure that no options are set, either via command-line or the `NODE_OPTIONS` environment variable, that would enable loader hooks. **CVE ID : CVE-2023-38704**		
Vendor: davidlingren					
Product: media_library_assistant					
Affected Version(s): * Up to (including) 3.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in submodule of David Lingren Media Library Assistant plugin <= 3.0.7 versions. **CVE ID : CVE-2023-34010**	N/A	A-DAV-MEDI-210823/574
Vendor: decondigital					
Product: decon_wp_sms					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Decon Digital Decon WP SMS plugin <= 1.1 versions. **CVE ID : CVE-2023-27416**	N/A	A-DEC-DECO-210823/575
Vendor: dedebiz					
Product: dedebiz					
Affected Version(s): 6.2.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	A vulnerability was found in DedeBIZ 6.2.10. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Article Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may	N/A	A-DED-DEDE-210823/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. VDB-236186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4170**		
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7.109					
Unrestricted Upload of File with Dangerous Type	03-Aug-2023	8.8	DedeCMS v5.7.109 has a File Upload vulnerability, leading to remote code execution (RCE). **CVE ID : CVE-2023-36298**	N/A	A-DED-DEDE-210823/577
Vendor: dieboldnixdorf					
Product: vynamic_view					
Affected Version(s): * Up to (including) 5.3.1					
Uncontrolled Search Path Element	08-Aug-2023	7.8	An issue in Diebold Nixdorf Vynamic View Console v.5.3.1 and before allows a local attacker to execute arbitrary code via not restricting the search path for required DLLs and not verifying the signature. **CVE ID : CVE-2023-36344**	https://www.dieboldnixdorf.com/en-us/banking/portfolio/software/view/	A-DIE-VYNA-210823/578
Vendor: digital-ant					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: digital_ant					
Affected Version(s): * Up to (excluding) 11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Digital Ant E-Commerce Software allows SQL Injection.This issue affects E-Commerce Software: before 11. **CVE ID : CVE-2023-3651**	N/A	A-DIG-DIGI-210823/579
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital Ant E-Commerce Software allows Reflected XSS.This issue affects E-Commerce Software: before 11. **CVE ID : CVE-2023-3652**	N/A	A-DIG-DIGI-210823/580
Improper Neutralization of Input During	08-Aug-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site	N/A	A-DIG-DIGI-210823/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in Digital Ant E-Commerce Software allows Stored XSS.This issue affects E-Commerce Software: before 11. **CVE ID : CVE-2023-3653**		
Vendor: doctors_appointment_system_project					
Product: doctors_appointment_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument useremail 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-236365 was assigned to this vulnerability. **CVE ID : CVE-2023-4219**	N/A	A-DOC-DOCT-210823/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: E107					
Product: e107					
Affected Version(s): 2.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	Cross Site Scripting vulnerability in e107 v.2.3.2 allows a remote attacker to execute arbitrary code via the description function in the SEO project. **CVE ID : CVE-2023-36121**	N/A	A-E10-E107-210823/583
Vendor: eggemplo					
Product: gestion-pymes					
Affected Version(s): * Up to (including) 1.5.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eggemplo Gestion-Pymes plugin <= 1.5.6 versions. **CVE ID : CVE-2023-38397**	N/A	A-EGG-GEST-210823/584
Product: woocommerce_email_report					
Affected Version(s): * Up to (including) 2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in eggemplo Woocommerce Email Report plugin <= 2.4 versions. **CVE ID : CVE-2023-27627**	N/A	A-EGG-WOOC-210823/585
Vendor: ehco1996					
Product: django-sspanel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2022.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Aug-2023	9.8	django-sspanel v2022.2.2 was discovered to contain a remote command execution (RCE) vulnerability via the component sspanel/admin_view.py -> GoodsCreateView._post. **CVE ID : CVE-2023-38941**	N/A	A-EHC-DJAN-210823/586
Vendor: elegant_themes					
Product: divi					
Affected Version(s): * Up to (including) 4.20.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Elegant themes Divi theme <= 4.20.2 versions. **CVE ID : CVE-2023-29099**	N/A	A-ELE-DIVI-210823/587
Vendor: element55					
Product: knowmore					
Affected Version(s): * Up to (excluding) 22					
Cleartext Storage of Sensitive Information	03-Aug-2023	7.5	Element55 KnowMore appliances version 21 and older was discovered to store passwords in plaintext. **CVE ID : CVE-2023-39144**	N/A	A-ELE-KNOW-210823/588
Vendor: emby					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: emby.releases					
Affected Version(s): 4.7.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	A vulnerability was found in Media Browser Emby Server 4.7.13.0 and classified as problematic. This issue affects some unknown processing of the file /web/. 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. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-236183. **CVE ID : CVE-2023-4167**	N/A	A-EMB-EMBY-210823/589
Vendor: emlog					
Product: emlog					
Affected Version(s): 2.1.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	7.2	emlog v2.1.9 was discovered to contain a SQL injection vulnerability via the component /admin/user.php. **CVE ID : CVE-2023-39121**	N/A	A-EML-EMLO-210823/590
Vendor: empowerid					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: empowerid					
Affected Version(s): * Up to (including) 7.205.0.0					
Insufficient Verification of Data Authenticity	06-Aug-2023	5.7	A vulnerability was found in EmpowerID up to 7.205.0.0. It has been rated as problematic. This issue affects some unknown processing of the component Multi-Factor Authentication Code Handler. The manipulation leads to information disclosure. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 7.205.0.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-236213 was assigned to this vulnerability. **CVE ID : CVE-2023-4177**	N/A	A-EMP-EMPO-210823/591
Vendor: ENG					
Product: knowage					
Affected Version(s): From (including) 6.1.0 Up to (excluding) 8.1.8					
Improper Limitation of a Pathname to a Restricted Directory	04-Aug-2023	8.8	Knowage is an open source analytics and business intelligence suite. Starting in the 6.x.x branch and prior to version 8.1.8, the endpoint	N/A	A-ENG-KNOW-210823/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			`/knowage/restful-services/dossier/importTemplateFile` allows authenticated users to upload `template file` on the server, but does not need any authorization to be reached. When the JSP file is uploaded, the attacker just needs to connect to `/knowageqbeengine/foo.jsp` to gain code execution on the server. By exploiting this vulnerability, an attacker with low privileges can upload a JSP file to the `knowageqbeengine` directory and gain code execution capability on the server. This issue has been patched in Knowage version 8.1.8. **CVE ID : CVE-2023-38702**		
Vendor: ens.domains					
Product: ethereum_name_service					
Affected Version(s): * Up to (excluding) 0.0.22					
Integer Overflow or Wraparound	04-Aug-2023	6.5	Ethereum Name Service (ENS) is a distributed, open, and extensible naming system based on the Ethereum blockchain.	https://github.com/ensdomains/ens-contracts/commit/e6b136e979084de3761c125142620304173990c	A-ENS-ETHE-210823/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			According to the documentation, controllers are allowed to register new domains and extend the expiry of existing domains, but they cannot change the ownership or reduce the expiration time of existing domains. However, a preliminary analysis suggests that an attacker-controlled controller may be able to reduce the expiration time of existing domains due to an integer overflow in the renew function. The vulnerability resides `@ensdomains/ens-contracts` prior to version 0.0.22. If successfully exploited, this vulnerability would enable attackers to force the expiration of any ENS record, ultimately allowing them to claim the affected domains for themselves. Currently, it would require a malicious DAO to exploit it. Nevertheless, any vulnerability present in the controllers could potentially	a, https://github.com/ensdomains/ens-contracts/security/advisories/GHSA-rrxv-q8m4-wch3	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			render this issue exploitable in the future. An additional concern is the possibility of renewal discounts. Should ENS decide to implement a system that offers unlimited .eth domains for a fixed fee in the future, the vulnerability could become exploitable by any user due to the reduced attack cost. Version 0.0.22 contains a patch for this issue. As long as registration cost remains linear or superlinear based on registration duration, or limited to a reasonable maximum (eg, 1 million years), this vulnerability could only be exploited by a malicious DAO. The interim workaround is thus to take no action. **CVE ID : CVE-2023-38698**		
Vendor: eramba					
Product: eramba					
Affected Version(s): 3.19.1					
Improper Control of Generation	03-Aug-2023	8.8	An issue in Eramba Limited Eramba Enterprise v.3.19.1	N/A	A-ERA-ERAM-210823/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			allows a remote attacker to execute arbitrary code via the path parameter in the URL. **CVE ID : CVE-2023-36255**		
Vendor: esds.co					
Product: emagic_data_center_management					
Affected Version(s): * Up to (including) 6.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	This vulnerability exists in ESDS Emagic Data Center Management Suit due to lack of input sanitization in its Ping component. A remote authenticated attacker could exploit this by injecting OS commands on the targeted system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on targeted system. **CVE ID : CVE-2023-37569**	N/A	A-ESD-EMAG-210823/595
Insufficient Session Expiration	08-Aug-2023	8.8	This vulnerability exists in ESDS Emagic Data Center Management Suit due to non-expiry of session cookie. By reusing the stolen cookie, a remote	N/A	A-ESD-EMAG-210823/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could gain unauthorized access to the targeted system. **CVE ID : CVE-2023-37570**		
Vendor: everestthemes					
Product: everest_news					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest themes Everest News theme <= 1.1.0 versions. **CVE ID : CVE-2023-27421**	N/A	A-EVE-EVER-210823/597
Product: mocho_blog					
Affected Version(s): * Up to (including) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest themes Mocho Blog theme <= 1.0.4 versions. **CVE ID : CVE-2023-27412**	N/A	A-EVE-MOCH-210823/598
Vendor: expresstech					
Product: quiz_and_survey_master					
Affected Version(s): * Up to (excluding) 8.1.11					
Improper Neutralization of Input During Web Page Generation	07-Aug-2023	5.4	The Quiz And Survey Master WordPress plugin before 8.1.11 does not properly sanitize and escape question titles, which could allow users with the Contributor	N/A	A-EXP-QUIZ-210823/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-3575**		
Vendor: F5					
Product: access_policy_manager_clients					
Affected Version(s): From (including) 7.2.3 Up to (excluding) 7.2.4.3					
Improper Verification of Cryptographic Signature	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**	https://my.f5.com/manage/s/article/K000134746	A-F5-ACCE-210823/600
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132563	A-F5-ACCE-210823/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36858		
Product: big-ip_access_policy_manager					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F.	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Verification of Cryptographic Signature	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions	https://my.f5.com/manage/s/article/K000134746	A-F5-BIG--210823/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/605
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	https://my.f5.com/manage/s/article/K000132563	A-F5-BIG--210823/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/607
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/608
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/610
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/612
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Improper Verification of Cryptographic Signature	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**	https://my.f5.com/manage/s/article/K000134746	A-F5-BIG--210823/613
Insufficient Verification of Data	02-Aug-2023	5.5	An insufficient verification of data	https://my.f5.com/manage/	A-F5-BIG--210823/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	s/article/K000132563	
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/615
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/617
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.9					
Improper Verification of Cryptographic Signature	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000134746	A-F5-BIG--210823/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**		
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	https://my.f5.com/manage/s/article/K000132563	A-F5-BIG--210823/619
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38138		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/621
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/622
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Improper Verification of	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not	https://my.f5.com/manage/	A-F5-BIG--210823/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**	s/article/K000134746	
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	https://my.f5.com/manage/s/article/K000132563	A-F5-BIG--210823/624
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/626
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38419		
Affected Version(s): From (including) 17.0.0 Up to (including) 17.1.0					
Improper Verification of Cryptographic Signature	02-Aug-2023	7.8	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38418**	https://my.f5.com/manage/s/article/K000134746	A-F5-BIG--210823/628
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	https://my.f5.com/manage/s/article/K000132563	A-F5-BIG--210823/629
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 15.1.0					
Weak Password	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS	https://my.f5.com/manage/	A-F5-BIG--210823/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requirements			HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.	s/article/K00 0135449	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38138		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/633
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/634
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS	https://my.f5.com/manage/	A-F5-BIG--210823/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requirements			HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.	s/article/K00 0135449	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/636
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/638
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38138		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/640
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/641
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists	https://my.f5.com/manage/	A-F5-BIG--210823/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	s/article/K000133474	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/643
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/645
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/647
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/650
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/652
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists	https://my.f5.com/manage/	A-F5-BIG--210823/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	s/article/K000133474	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/655
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/657
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/659
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/661
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/662
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/663
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/664
Improper Handling of Exceptiona	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Product: big-ip_analytics					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest.	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/668
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/670
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/673
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38419		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/675
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/677
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/678
Improper Neutralization of Input During	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/680
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/682
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Product: big-ip_application_acceleration_manager					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/687
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/691
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/692
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/694
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note:	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/696
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/698
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/700
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/701
Product: big-ip_application_security_manager					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/705
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/706
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/708
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/710
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/712
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/713
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/715
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/717
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/719
Product: big-ip_application_visibility_and_reporting					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS	https://my.f5.com/manage/	A-F5-BIG--210823/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requirements			HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.	s/article/K00 0135449	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/722
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/724
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/727
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/729
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/731
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/733
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/734
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/736
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Product: big-ip_carrier-grade_nat					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-	https://my.f5.com/manage/s/article/K00135449	A-F5-BIG--210823/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/741
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/745
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/746
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/748
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/750
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/752
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/754
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/755
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): 15.1.0					
Weak Password	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate	https://my.f5.com/manage/	A-F5-BIG--210823/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requirements			a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.	s/article/K00 0135449	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/759
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/760
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/762
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/764
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/766
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/767
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/769
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/771
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/773
Product: big-ip_domain_name_system					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/776
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/778
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/780
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/782
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/783
Improper Neutralization of Input During	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/785
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/787
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/789
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/791
Product: big-ip_edge_gateway					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/794
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38423		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/796
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/799
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/801
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/803
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/805
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/806
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/808
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Product: big-ip_fraud_protection_service					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/813
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/817
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/818
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/820
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note:	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/822
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/824
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38138		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/826
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/827
Product: big-ip_global_traffic_manager					
Affected Version(s): 15.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/831
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/832
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/834
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/836
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/838
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/840
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/842
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/843
Improper Neutralization of Input During	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/845
Product: big-ip_link_controller					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F.	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/848
Improper Neutralization of Input	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of	https://my.f5.com/manage/	A-F5-BIG--210823/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	s/article/K00 0134535	
Improper Handling of Exceptiona l Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5. com/manage/ s/article/K00 0133472	A-F5-BIG-- 210823/850
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requireme nts	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows	https://my.f5. com/manage/ s/article/K00 0135449	A-F5-BIG-- 210823/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/852
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38423		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/854
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/855
Improper Neutralization of Input	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/857
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/859
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38419		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/861
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/863
Product: big-ip_local_traffic_manager					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/866
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/868
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/871
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/873
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/875
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/876
Improper Neutralization of Input During	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/878
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/880
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/885
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/889
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/890
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/892
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note:	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/894
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/896
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/898
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/899
Product: big-ip_ssl_orchestrator					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F,	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/903
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/904
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/906
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/908
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/910
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/911
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/913
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/915
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/917
Product: big-ip_webaccelerator					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/920
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38423		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/922
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/925
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38419		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/927
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/929
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/930
Improper Neutralization of Input During Web Page	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/932
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/934
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: big-ip_websafe					
Affected Version(s): 15.1.0					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (excluding) 13.1.4					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest.	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/939
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/940
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS	https://my.f5.com/manage/s/article/K000135449	A-F5-BIG--210823/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/942
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/944
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38138		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/946
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/947
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.5					
Improper Neutralization of Input	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38423**	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/949
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note:	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38138**	https://my.f5.com/manage/s/article/K000133474	A-F5-BIG--210823/951
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000134535	A-F5-BIG--210823/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-38423**		
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/953
Product: big-iq_centralized_management					
Affected Version(s): From (including) 8.2.0 Up to (including) 8.3.0					
Improper Handling of Exceptional Conditions	02-Aug-2023	4.3	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-38419**	https://my.f5.com/manage/s/article/K000133472	A-F5-BIG--210823/954
Product: f5os-a					
Affected Version(s): 1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	02-Aug-2023	4.4	Audit logs on F5OS-A may contain undisclosed sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36494**	https://my.f5.com/manage/s/article/K000134922	A-F5-F5OS-210823/955
Vendor: Fabasoft					
Product: cloud					
Affected Version(s): -					
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	A-FAB-CLOU-210823/956
Product: cloud_enterprise_client					
Affected Version(s): 23.3.0.130					
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-	A-FAB-CLOU-210823/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	
Product: folio_\/_egov-suite					
Affected Version(s): 2021					
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	A-FAB-FOLI-210823/958
Affected Version(s): 2022					
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	A-FAB-FOLI-210823/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2023					
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	A-FAB-FOLI-210823/960
Vendor: faculty_evaulation_system_project					
Product: faculty_evaulation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	5.4	Cross Site Scripting vulnerability in Faculty Evaulation System using PHP/MySQLi v.1.0 allows an attacker to execute arbitrary code via a crafted payload to the page parameter. **CVE ID : CVE-2023-36118**	N/A	A-FAC-FACU-210823/961
Vendor: farmakom					
Product: remote_administration_console					
Affected Version(s): * Up to (excluding) 1.02					
Improper Neutralization of Special Elements	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL	N/A	A-FAR-REMO-210823/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection') vulnerability in Farmakom Remote Administration Console allows SQL Injection.This issue affects Remote Administration Console: before 1.02. **CVE ID : CVE-2023-3717**		
Vendor: Fasterxml					
Product: jackson-dataformats-text					
Affected Version(s): * Up to (excluding) 2.15.0					
Out-of-bounds Write	08-Aug-2023	7.5	Those using jackson-dataformats-text to parse TOML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2023-3894**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50083, https://github.com/FasterXML/jackson-dataformats-text/pull/398	A-FAS-JACK-210823/963
Vendor: fit2cloud					
Product: cloudexplorer_lite					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Special Elements used in an	04-Aug-2023	9.8	CloudExplorer Lite is an open source, lightweight cloud management platform. Versions prior to 1.3.1 contain	N/A	A-FIT-CLOU-210823/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			a command injection vulnerability in the installation function in module management. The vulnerability has been fixed in v1.3.1. There are no known workarounds aside from upgrading. **CVE ID : CVE-2023-38692**		
Vendor: fobybus					
Product: social-media-skeleton					
Affected Version(s): * Up to (excluding) 1.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	social-media-skeleton is an uncompleted social media project implemented using PHP, MySQL, CSS, JavaScript, and HTML. Versions 1.0.0 until 1.0.3 have a stored cross-site scripting vulnerability. The problem is patched in v1.0.3. **CVE ID : CVE-2023-39518**	https://github.com/fobybus/social-media-skeleton/pull/4, https://github.com/fobybus/social-media-skeleton/security/advisories/GHSA-2jxx-r967-f76p, https://github.com/fobybus/social-media-skeleton/commit/676d1109016e1f1d707ef47917927c7704e6428	A-FOB-SOCI-210823/965
Affected Version(s): 1.0.0					
Improper Neutralization of Special Elements used in an	04-Aug-2023	8.8	social-media-skeleton is an uncompleted social media project. A SQL injection vulnerability in the	https://github.com/fobybus/social-media-skeleton/security/advisories/GHSA-857x-	A-FOB-SOCI-210823/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			project allows UNION based injections, which indirectly leads to remote code execution. Commit 3cabdd35c3d874608883c9eaf9bf69b2014d25c1 contains a fix for this issue. **CVE ID : CVE-2023-39344**	p6fq-mgfh, https://github.com/fobybus/social-media-skeleton/commit/3cabdd35c3d874608883c9eaf9bf69b2014d25c1	
Vendor: Foswiki					
Product: foswiki					
Affected Version(s): From (including) 1.0.0 Up to (including) 2.1.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Aug-2023	7.5	An issue in the SpreadSheetPlugin component of Foswiki v2.1.7 and below allows attackers to execute a directory traversal. **CVE ID : CVE-2023-33756**	https://foswiki.org/Support/SecurityAlert-CVE-2023-33756	A-FOS-FOSW-210823/967
Affected Version(s): From (including) 2.0.0 Up to (including) 2.1.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Aug-2023	7.5	Insufficient parameter validation in the Foswiki::Sandbox component of Foswiki v2.1.7 and below allows attackers to perform a directory traversal via supplying a crafted web request. **CVE ID : CVE-2023-24698**	https://foswiki.org/Support/SecurityAlert-CVE-2023-24698	A-FOS-FOSW-210823/968
Vendor: Fujitsu					
Product: software_infrastructure_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.8.0.061					
Cleartext Storage of Sensitive Information	07-Aug-2023	5	An issue was discovered in Fujitsu Software Infrastructure Manager (ISM) before 2.8.0.061. The ismsnap component (in this specific case at /var/log/fujitsu/ServerViewSuite/ism/FirmwareManagement/FirmwareManagement.log) allows insecure collection and storage of authorization credentials in cleartext. That occurs when users perform any ISM Firmware Repository Address setup test (Test the Connection), or regularly authorize against an already configured remote firmware repository site, as set up in ISM Firmware Repository Address. A privileged attacker is therefore able to potentially gather the associated ismsnap maintenance data, in the same manner as a trusted party allowed to export ismsnap data from ISM. The preconditions for an	https://security.ts.fujitsu.com/ProductSecurity/content/Fujitsu-PSIRT-ISS-IS-2023-071410-Security-Notice.pdf, https://security.ts.fujitsu.com/IndexDownload.asp?SoftwareGuid=a0131919-6d84-43b4-800e-d7f78200a70f	A-FUJ-SOFT-210823/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISM installation to be generally vulnerable are that the Download Firmware (Firmware Repository Server) function is enabled and configured, and that the character \ (backslash) is used in a user credential (i.e., user/ID or password) of the remote proxy host / firmware repository server. NOTE: this may overlap CVE-2023-39379. **CVE ID : CVE-2023-39903**		
Affected Version(s): 2.8.0.060					
Cleartext Storage of Sensitive Informatio n	04-Aug-2023	7.5	Fujitsu Software Infrastructure Manager (ISM) stores sensitive information at the product's maintenance data (ismsnap) in cleartext form. As a result, the password for the proxy server that is configured in ISM may be retrieved. Affected products and versions are as follows: Fujitsu Software Infrastructure Manager Advanced Edition V2.8.0.060, Fujitsu Software	N/A	A-FUJ-SOFT-210823/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure Manager Advanced Edition for PRIMEFLEX V2.8.0.060, and Fujitsu Software Infrastructure Manager Essential Edition V2.8.0.060. **CVE ID : CVE-2023-39379**		
Vendor: full					
Product: full_-_customer					
Affected Version(s): * Up to (including) 2.2.3					
Unrestricted Upload of File with Dangerous Type	09-Aug-2023	8.8	The FULL - Customer plugin for WordPress is vulnerable to Arbitrary File Upload via the /install-plugin REST route in versions up to, and including, 2.2.3 due to improper authorization. This allows authenticated attackers with subscriber-level permissions and above to execute code by installing plugins from arbitrary remote locations including non-repository sources onto the site, granted they are packaged as a valid WordPress plugin. **CVE ID : CVE-2023-4243**	N/A	A-FUL-FULL-210823/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	09-Aug-2023	4.3	The FULL - Customer plugin for WordPress is vulnerable to Information Disclosure via the /health REST route in versions up to, and including, 2.2.3 due to improper authorization. This allows authenticated attackers with subscriber-level permissions and above to obtain sensitive information about the site configuration as disclosed by the WordPress health check. **CVE ID : CVE-2023-4242**	N/A	A-FUL-FULL-210823/972
Vendor: getbutton					
Product: chat_button					
Affected Version(s): * Up to (excluding) 1.8.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GetButton Chat Button by GetButton.Io plugin <= 1.8.9.4 versions. **CVE ID : CVE-2023-32292**	N/A	A-GET-CHAT-210823/973
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 16.0.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. The main branch of a repository with a specially designed name allows an attacker to create repositories with malicious code. **CVE ID : CVE-2023-3401**	N/A	A-GIT-GITL-210823/974
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2, which leads to developers being able to create pipeline schedules on protected branches even if they don't have access to merge **CVE ID : CVE-2023-2022**	N/A	A-GIT-GITL-210823/975
Affected Version(s): From (including) 10.0 Up to (excluding) 16.0.8					
Improper Neutralization of Input	02-Aug-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting	N/A	A-GIT-GITL-210823/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			from 10.0 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A reflected XSS was possible when creating specific PlantUML diagrams that allowed the attacker to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-3500**		
Affected Version(s): From (including) 12.9 Up to (excluding) 16.0.8					
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 12.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to leak a user's email via an error message for groups that restrict membership by email domain. **CVE ID : CVE-2023-1210**	N/A	A-GIT-GITL-210823/977
Affected Version(s): From (including) 13.12.0 Up to (excluding) 16.0.8					
N/A	03-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before	N/A	A-GIT-GITL-210823/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to run pipeline jobs as an arbitrary user via scheduled security scan policies. **CVE ID : CVE-2023-3932**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 16.0.8					
N/A	04-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.1 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for EE-licensed users to link any security policy project by its ID to projects or groups the user has access to, potentially revealing the security projects's configured security policies. **CVE ID : CVE-2023-4002**	N/A	A-GIT-GITL-210823/979
Affected Version(s): From (including) 14.3 Up to (excluding) 16.0.8					
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab	N/A	A-GIT-GITL-210823/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EE affecting all versions starting from 14.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Access tokens may have been logged when a query was made to a specific endpoint. **CVE ID : CVE-2023-3993**		
Affected Version(s): From (including) 15.11 Up to (excluding) 16.2.2					
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab EE affecting all versions from 15.11 prior to 16.2.2 which allows an attacker to spike the resource consumption resulting in DoS. **CVE ID : CVE-2023-4011**	N/A	A-GIT-GITL-210823/981
Affected Version(s): From (including) 15.2 Up to (excluding) 16.0.8					
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible by using crafted payloads to	N/A	A-GIT-GITL-210823/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			search Harbor Registry. **CVE ID : CVE-2023-0632**		
Affected Version(s): From (including) 15.9 Up to (excluding) 16.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to trigger a stored XSS vulnerability via user interaction with a crafted URL in the WebIDE beta. **CVE ID : CVE-2023-2164**	N/A	A-GIT-GITL-210823/983
Affected Version(s): From (including) 15.9.0 Up to (excluding) 16.0.8					
N/A	03-Aug-2023	9.8	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to takeover GitLab Pages with unique domain URLs if the random string added was known.	N/A	A-GIT-GITL-210823/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4008		
Affected Version(s): From (including) 16.1 Up to (excluding) 16.1.3					
N/A	03-Aug-2023	9.8	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to takeover GitLab Pages with unique domain URLs if the random string added was known. **CVE ID : CVE-2023-4008**	N/A	A-GIT-GITL-210823/985
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible by using crafted payloads to search Harbor Registry. **CVE ID : CVE-2023-0632**	N/A	A-GIT-GITL-210823/986
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all	N/A	A-GIT-GITL-210823/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 8.14 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use AutolinkFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3364**		
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. An invalid 'start_sha' value on merge requests page may lead to Denial of Service as Changes tab would not load. **CVE ID : CVE-2023-3900**	N/A	A-GIT-GITL-210823/988
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before	N/A	A-GIT-GITL-210823/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.2.2. Access tokens may have been logged when a query was made to a specific endpoint. **CVE ID : CVE-2023-3993**		
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use ProjectReferenceFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3994**	N/A	A-GIT-GITL-210823/990
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 8.10 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Under specific circumstances, a user importing a project 'from export' could access and	N/A	A-GIT-GITL-210823/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read unrelated files via uploading a specially crafted file. This was due to a bug in `tar`, fixed in [`tar-1.35`](https://lists.gnu.org/archive/html/info-gnu/2023-07/msg00005.html). **CVE ID : CVE-2023-3385**		
Improper Control of Generation of Code ('Code Injection')	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. The main branch of a repository with a specially designed name allows an attacker to create repositories with malicious code. **CVE ID : CVE-2023-3401**	N/A	A-GIT-GITL-210823/992
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.0 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A reflected XSS was possible when creating	N/A	A-GIT-GITL-210823/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific PlantUML diagrams that allowed the attacker to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-3500**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to trigger a stored XSS vulnerability via user interaction with a crafted URL in the WebIDE beta. **CVE ID : CVE-2023-2164**	N/A	A-GIT-GITL-210823/994
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 12.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to leak a user's email via an error message for groups that restrict	N/A	A-GIT-GITL-210823/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			membership by email domain. **CVE ID : CVE-2023-1210**		
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2, which leads to developers being able to create pipeline schedules on protected branches even if they don't have access to merge **CVE ID : CVE-2023-2022**	N/A	A-GIT-GITL-210823/996
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
N/A	03-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to run pipeline jobs as an arbitrary user via scheduled security scan policies.	N/A	A-GIT-GITL-210823/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3932		
N/A	04-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.1 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for EE-licensed users to link any security policy project by its ID to projects or groups the user has access to, potentially revealing the security projects's configured security policies. **CVE ID : CVE-2023-4002**	N/A	A-GIT-GITL-210823/998
Affected Version(s): From (including) 16.2 Up to (excluding) 16.2.2					
N/A	03-Aug-2023	9.8	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to takeover GitLab Pages with unique domain URLs	N/A	A-GIT-GITL-210823/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if the random string added was known. **CVE ID : CVE-2023-4008**		
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible by using crafted payloads to search Harbor Registry. **CVE ID : CVE-2023-0632**	N/A	A-GIT-GITL-210823/1000
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.14 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use AutolinkFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3364**	N/A	A-GIT-GITL-210823/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. An invalid 'start_sha' value on merge requests page may lead to Denial of Service as Changes tab would not load. **CVE ID : CVE-2023-3900**	N/A	A-GIT-GITL-210823/1002
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Access tokens may have been logged when a query was made to a specific endpoint. **CVE ID : CVE-2023-3993**	N/A	A-GIT-GITL-210823/1003
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before	N/A	A-GIT-GITL-210823/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use ProjectReferenceFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3994**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 8.10 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Under specific circumstances, a user importing a project 'from export' could access and read unrelated files via uploading a specially crafted file. This was due to a bug in `tar`, fixed in [`tar-1.35`](https://lists.gnu.org/archive/html/info-gnu/2023-07/msg00005.html). **CVE ID : CVE-2023-3385**	N/A	A-GIT-GITL-210823/1005
Improper Control of Generation of Code	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions before 16.0.8, all versions starting	N/A	A-GIT-GITL-210823/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. The main branch of a repository with a specially designed name allows an attacker to create repositories with malicious code. **CVE ID : CVE-2023-3401**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.0 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A reflected XSS was possible when creating specific PlantUML diagrams that allowed the attacker to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-3500**	N/A	A-GIT-GITL-210823/1007
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2	N/A	A-GIT-GITL-210823/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			before 16.2.2. It was possible for an attacker to trigger a stored XSS vulnerability via user interaction with a crafted URL in the WebIDE beta. **CVE ID : CVE-2023-2164**		
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 12.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to leak a user's email via an error message for groups that restrict membership by email domain. **CVE ID : CVE-2023-1210**	N/A	A-GIT-GITL-210823/1009
N/A	02-Aug-2023	4.3	An issue has been discovered in GitLab CE/EE affecting all versions starting before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2, which leads to developers being able to create pipeline schedules on protected branches even if they	N/A	A-GIT-GITL-210823/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			don't have access to merge **CVE ID : CVE-2023-2022**		
Affected Version(s): From (including) 16.2.0 Up to (excluding) 16.2.2					
N/A	03-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to run pipeline jobs as an arbitrary user via scheduled security scan policies. **CVE ID : CVE-2023-3932**	N/A	A-GIT-GITL-210823/1011
N/A	04-Aug-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.1 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for EE-licensed users to link any security policy project by its ID to projects or groups the user has access to, potentially	N/A	A-GIT-GITL-210823/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			revealing the security projects's configured security policies. **CVE ID : CVE-2023-4002**		
Affected Version(s): From (including) 8.10 Up to (excluding) 16.0.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 8.10 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Under specific circumstances, a user importing a project 'from export' could access and read unrelated files via uploading a specially crafted file. This was due to a bug in `tar`, fixed in [`tar-1.35`](https://lists.gnu.org/archive/html/info-gnu/2023-07/msg00005.html). **CVE ID : CVE-2023-3385**	N/A	A-GIT-GITL-210823/1013
Affected Version(s): From (including) 8.14 Up to (excluding) 16.0.8					
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.14 before 16.0.8, all versions starting from 16.1	N/A	A-GIT-GITL-210823/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use AutolinkFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3364**		
Affected Version(s): From (including) 9.3 Up to (excluding) 16.0.8					
N/A	02-Aug-2023	7.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use ProjectReferenceFilter to the preview_markdown endpoint. **CVE ID : CVE-2023-3994**	N/A	A-GIT-GITL-210823/1015
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.19.12					
Allocation of Resources	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p	https://github.com/libp2p/go-	A-GOL-GO-210823/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no known workarounds for this issue. **CVE ID : CVE-2023-39533**	libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/go-libp2p/security/advisories/GHSA-876p-8259-xjgg	
Uncontrolled Resource Consumption	02-Aug-2023	5.3	Extremely large RSA keys in certificate chains can cause a client/server to expend significant	https://go.dev/cl/515257, https://groups.google.com/g/golang-	A-GOL-GO-210823/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU time verifying signatures. With fix, the size of RSA keys transmitted during handshakes is restricted to <= 8192 bits. Based on a survey of publicly trusted RSA keys, there are currently only three certificates in circulation with keys larger than this, and all three appear to be test certificates that are not actively deployed. It is possible there are larger keys in use in private PKIs, but we target the web PKI, so causing breakage here in the interests of increasing the default safety of users of crypto/tls seems reasonable. **CVE ID : CVE-2023-29409**	announce/c/X0b6CsSAaYI/m/Efv5DbZ9AwAJ, https://pkg.go.dev/vuln/GO-2023-1987, https://go.dev/issue/61460	
Affected Version(s): 1.21.0					
Uncontrolled Resource Consumption	02-Aug-2023	5.3	Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures. With fix, the size of RSA keys transmitted during handshakes is restricted to <= 8192 bits. Based on a	https://go.dev/cl/515257, https://groups.google.com/g/golang-announce/c/X0b6CsSAaYI/m/Efv5DbZ9AwAJ, https://pkg.go.dev/vuln/GO-2023-1987,	A-GOL-GO-210823/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			survey of publicly trusted RSA keys, there are currently only three certificates in circulation with keys larger than this, and all three appear to be test certificates that are not actively deployed. It is possible there are larger keys in use in private PKIs, but we target the web PKI, so causing breakage here in the interests of increasing the default safety of users of crypto/tls seems reasonable. **CVE ID : CVE-2023-29409**	https://go.dev/issue/61460	
Affected Version(s): From (including) 1.20.0 Up to (excluding) 1.20.7					
Allocation of Resources Without Limits or Throttling	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can	https://github.com/libp2p/go-libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/g	A-GOL-GO-210823/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no known workarounds for this issue. **CVE ID : CVE-2023-39533**	o-libp2p/security/advisories/GHSA-876p-8259-xjgg	
Uncontrolled Resource Consumption	02-Aug-2023	5.3	Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures. With fix, the size of RSA keys transmitted during handshakes is restricted to <= 8192 bits. Based on a survey of publicly trusted RSA keys, there are currently only three certificates in circulation with keys larger than this, and all three appear to be test certificates that	https://go.dev/cl/515257, https://groups.google.com/g/golang-announce/c/X0b6CsSAaYI/m/Efv5DbZ9AwAJ, https://pkg.go.dev/vuln/GO-2023-1987, https://go.dev/issue/61460	A-GOL-GO-210823/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are not actively deployed. It is possible there are larger keys in use in private PKIs, but we target the web PKI, so causing breakage here in the interests of increasing the default safety of users of crypto/tls seems reasonable. **CVE ID : CVE-2023-29409**		
Product: image					
Affected Version(s): * Up to (excluding) 0.10.0					
Excessive Iteration	02-Aug-2023	6.5	A maliciously-crafted image can cause excessive CPU consumption in decoding. A tiled image with a height of 0 and a very large width can cause excessive CPU consumption, despite the image size (width * height) appearing to be zero. **CVE ID : CVE-2023-29407**	https://go.dev/cl/514897, https://go.dev/issue/61581, https://pkg.go.dev/vuln/GO-2023-1990	A-GOL-IMAG-210823/1021
Allocation of Resources Without Limits or Throttling	02-Aug-2023	6.5	The TIFF decoder does not place a limit on the size of compressed tile data. A maliciously-crafted image can exploit this to cause a small image (both in terms of pixel width/height, and encoded size) to	https://pkg.go.dev/vuln/GO-2023-1989, https://go.dev/cl/514897, https://go.dev/issue/61582	A-GOL-IMAG-210823/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make the decoder decode large amounts of compressed data, consuming excessive memory and CPU. **CVE ID : CVE-2023-29408**		
Product: networking					
Affected Version(s): * Up to (excluding) 0.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	Text nodes not in the HTML namespace are incorrectly literally rendered, causing text which should be escaped to not be. This could lead to an XSS attack. **CVE ID : CVE-2023-3978**	https://go.dev/issue/61615, https://go.dev/cl/514896, https://pkg.go.dev/vuln/GO-2023-1988	A-GOL-NETW-210823/1023
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 115.0.5790.131					
Use After Free	01-Aug-2023	8.8	Use after free in Diagnostics in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) **CVE ID : CVE-2023-3731**	https://crbug.com/1441306, https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-chromeos.html	A-GOO-CHRO-210823/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	6.3	Insufficient validation of untrusted input in Chromad in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker to execute arbitrary code via a crafted shell script. (Chromium security severity: Low) **CVE ID : CVE-2023-3739**	https://crbug.com/1398986, https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-chromeos.html	A-GOO-CHRO-210823/1025
Affected Version(s): * Up to (excluding) 115.0.5790.170					
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-2023	8.8	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4069**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1026
Out-of-bounds Write	03-Aug-2023	8.8	Heap buffer overflow in Visuals in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4071**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	03-Aug-2023	8.8	Out of bounds read and write in WebGL in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4072**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1028
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2023	8.8	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4073**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1029
Use After Free	03-Aug-2023	8.8	Use after free in Blink Task Scheduling in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4074**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Aug-2023	8.8	Use after free in Cast in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4075**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1031
Use After Free	03-Aug-2023	8.8	Use after free in WebRTC in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC session. (Chromium security severity: High) **CVE ID : CVE-2023-4076**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1032
N/A	03-Aug-2023	8.8	Insufficient data validation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension.	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Medium) **CVE ID : CVE-2023-4077**		
N/A	03-Aug-2023	8.8	Inappropriate implementation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium) **CVE ID : CVE-2023-4078**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1034
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-2023	8.1	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4068**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1035
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-2023	8.1	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-210823/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4070**		
Affected Version(s): * Up to (excluding) 115.0.5790.98					
Use After Free	01-Aug-2023	8.8	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3727**	https://crbug.com/1454086	A-GOO-CHRO-210823/1037
Use After Free	01-Aug-2023	8.8	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3728**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1457421	A-GOO-CHRO-210823/1038
Use After Free	01-Aug-2023	8.8	Use after free in Splitscreen in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker who convinced a user to engage in specific UI	https://crbug.com/1451803	A-GOO-CHRO-210823/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interactions to potentially exploit heap corruption via crafted UI interactions. (Chromium security severity: High) **CVE ID : CVE-2023-3729**		
Use After Free	01-Aug-2023	8.8	Use after free in Tab Groups in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-3730**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1453465	A-GOO-CHRO-210823/1040
Out-of-bounds Write	01-Aug-2023	8.8	Out of bounds memory access in Mojo in Google Chrome prior to 115.0.5790.98 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-2023-3732**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1450899	A-GOO-CHRO-210823/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Aug-2023	4.3	Inappropriate implementation in WebApp Installs in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-3733**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1450203	A-GOO-CHRO-210823/1042
N/A	01-Aug-2023	4.3	Inappropriate implementation in Picture In Picture in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-3734**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1450376	A-GOO-CHRO-210823/1043
N/A	01-Aug-2023	4.3	Inappropriate implementation in Web API Permission Prompts in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page.	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1394410	A-GOO-CHRO-210823/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Medium) **CVE ID : CVE-2023-3735**		
N/A	01-Aug-2023	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 115.0.5790.98 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-3736**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1434438	A-GOO-CHRO-210823/1045
N/A	01-Aug-2023	4.3	Inappropriate implementation in Notifications in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to spoof the contents of media notifications via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-3737**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1446754	A-GOO-CHRO-210823/1046
N/A	01-Aug-2023	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page.	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1434330	A-GOO-CHRO-210823/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Medium) **CVE ID : CVE-2023-3738**		
N/A	01-Aug-2023	4.3	Insufficient validation of untrusted input in Themes in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially serve malicious content to a user via a crafted background URL. (Chromium security severity: Low) **CVE ID : CVE-2023-3740**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1405223	A-GOO-CHRO-210823/1048
Vendor: greenshot					
Product: greenshot					
Affected Version(s): * Up to (including) 1.2.10					
N/A	01-Aug-2023	7.8	Greenshot 1.2.10 and below allows arbitrary code execution because .NET content is insecurely deserialized when a .greenshot file is opened. **CVE ID : CVE-2023-34634**	https://github.com/greenshot/greenshot/commit/a152e2883fca7f78051b3bd6b1e5cc57355cb44c	A-GRE-GREE-210823/1049
Vendor: gtmetrix					
Product: gtmetrix					
Affected Version(s): * Up to (including) 0.4.6					
Improper Neutralization of	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in	N/A	A-GTM-GTME-210823/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			GTmetrix GTmetrix for WordPress plugin <= 0.4.6 versions. **CVE ID : CVE-2023-32503**		
Vendor: hcltech					
Product: dryice_mycloud					
Affected Version(s): 10.2					
Use of a Broken or Risky Cryptographic Algorithm	09-Aug-2023	7.1	HCL DRYiCE MyCloud is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information. **CVE ID : CVE-2023-23346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106670	A-HCL-DRYI-210823/1051
Affected Version(s): 10.4					
Use of a Broken or Risky Cryptographic Algorithm	09-Aug-2023	7.1	HCL DRYiCE MyCloud is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information. **CVE ID : CVE-2023-23346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106670	A-HCL-DRYI-210823/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.5					
Use of a Broken or Risky Cryptographic Algorithm	09-Aug-2023	7.1	HCL DRYiCE MyCloud is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information. **CVE ID : CVE-2023-23346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106670	A-HCL-DRYI-210823/1053
Affected Version(s): 10.6					
Use of a Broken or Risky Cryptographic Algorithm	09-Aug-2023	7.1	HCL DRYiCE MyCloud is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information. **CVE ID : CVE-2023-23346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106670	A-HCL-DRYI-210823/1054
Product: unica					
Affected Version(s): * Up to (excluding) 11.1.0.6					
Improper Restriction of XML External Entity Reference	03-Aug-2023	8.8	The Unica application exposes an API which accepts arbitrary XML input. By manipulating the given XML, an authenticated	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106547	A-HCL-UNIC-210823/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with certain rights can successfully perform XML External Entity attacks (XXE) against the backend service. **CVE ID : CVE-2023-37497**		
Affected Version(s): * Up to (excluding) 12.1.1					
N/A	03-Aug-2023	8.8	A user is capable of assigning him/herself to arbitrary groups by reusing a POST request issued by an administrator. It is possible that an attacker could potentially escalate their privileges. **CVE ID : CVE-2023-37498**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106545	A-HCL-UNIC-210823/1056
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A Persistent Cross-site Scripting (XSS) vulnerability can be carried out in a certain field of the Unica Platform. An attacker could hijack a user's session and perform other attacks. **CVE ID : CVE-2023-37499**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106555	A-HCL-UNIC-210823/1057
Improper Neutralization of Input	03-Aug-2023	6.1	A Persistent Cross-site Scripting (XSS) vulnerability can be carried out on	https://support.hcltechsw.com/csm?id=kb_article&sysp	A-HCL-UNIC-210823/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			certain pages of Unica Platform. An attacker could hijack a user's session and perform other attacks. **CVE ID : CVE-2023-37500**	arm_article=KB0106554	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A Persistent XSS vulnerability can be carried out in a certain field of Unica Campaign. An attacker could hijack a user's session and perform other attacks. **CVE ID : CVE-2023-37501**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106556	A-HCL-UNIC-210823/1059
Affected Version(s): From (including) 12.0 Up to (excluding) 12.1.1					
Improper Restriction of XML External Entity Reference	03-Aug-2023	8.8	The Unica application exposes an API which accepts arbitrary XML input. By manipulating the given XML, an authenticated attacker with certain rights can successfully perform XML External Entity attacks (XXE) against the backend service. **CVE ID : CVE-2023-37497**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106547	A-HCL-UNIC-210823/1060
Product: verse					
Affected Version(s): * Up to (excluding) 3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	5.4	HCL Verse is susceptible to a Stored Cross Site Scripting (XSS) vulnerability. An attacker could execute script in a victim's web browser to perform operations as the victim and/or steal the victim's cookies, session tokens, or other sensitive information. **CVE ID : CVE-2023-37496**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0105904	A-HCL-VERS-210823/1061
Vendor: hedgedoc					
Product: hedgedoc					
Affected Version(s): * Up to (excluding) 1.9.9					
Authentication Bypass by Alternate Name	04-Aug-2023	8.2	HedgeDoc is software for creating real-time collaborative markdown notes. Prior to version 1.9.9, the API of HedgeDoc 1 can be used to create notes with an alias matching the ID of existing notes. The affected existing note can then not be accessed anymore and is effectively hidden by the new one. When the freeURL feature is enabled (by setting the `allowFreeURL`	https://github.com/hedgedoc/hedgedoc/pull/4476/commits/781263ab84255885e1fe60c7e92e2f8d611664d2, https://github.com/hedgedoc/hedgedoc/security/advisories/GHSA-7494-7hcf-vxpg	A-HED-HEDG-210823/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			config option or the `CMD_ALLOW_FREE URL` environment variable to `true`), any user with the appropriate permissions can create a note by making a POST request to the `/new/<ALIAS>` API endpoint. The `<ALIAS>` parameter can be set to the ID of an existing note. HedgeDoc did not verify whether the provided `<ALIAS>` value corresponds to a valid ID of an existing note and always allowed creation of the new note. When a visitor tried to access the existing note, HedgeDoc will first search for a note with a matching alias before it searches using the ID, therefore only the new note can be accessed. Depending on the permission settings of the HedgeDoc instance, the issue can be exploited only by logged-in users or by all (including non-logged-in) users. The exploit requires knowledge of the ID		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the target note. Attackers could use this issue to present a manipulated copy of the original note to the user, e.g. by replacing the links with malicious ones. Attackers can also use this issue to prevent access to the original note, causing a denial of service. No data is lost, as the original content of the affected notes is still present in the database. This issue was fixed in version 1.9.9. As a workaround, disabling freeURL mode prevents the exploitation of this issue. The impact can be limited by restricting freeURL note creation to trusted, logged-in users by enabling `requireFreeURLAuthentication`/`CMD_REQUIRE_FREEURL_AUTHENTICATION`. **CVE ID : CVE-2023-38487**		
Vendor: hikashop					
Product: hikashop					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.7.2					
Improper Neutralization of	07-Aug-2023	9.8	Improper Neutralization of Special Elements	N/A	A-HIK-HIKA-210823/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection. **CVE ID : CVE-2023-38044**		
Vendor: hospital_management_system_project					
Product: hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2023	9.8	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file appointmentapproval.php. The manipulation of the argument time 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-236211. **CVE ID : CVE-2023-4176**	N/A	A-HOS-HOSP-210823/1064
Vendor: i13websolution					
Product: wordpress_vertical_image_slider					
Affected Version(s): * Up to (excluding) 1.2.17					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution WordPress vertical image slider plugin <= 1.2.16 versions. **CVE ID : CVE-2023-24413**	N/A	A-I13-WORD-210823/1065
Product: wp_responsive_tabs_horizontal_vertical_and_accordion_tabs					
Affected Version(s): * Up to (excluding) 1.1.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution WP Responsive Tabs horizontal vertical and accordion Tabs plugin <= 1.1.15 versions. **CVE ID : CVE-2023-24409**	N/A	A-I13-WP_R-210823/1066
Vendor: IBM					
Product: robotic_process_automation					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 23.0.0					
Incorrect Authorization	02-Aug-2023	6.5	IBM Robotic Process Automation 21.0.0 through 21.0.7.latest is vulnerable to unauthorized access to data due to insufficient authorization validation on some API routes. IBM X-Force ID: 245425. **CVE ID : CVE-2023-23476**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245425, https://www.ibm.com/support/pages/node/7017490	A-IBM-ROBO-210823/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 23.0.0					
Incorrect Authorization	02-Aug-2023	6.5	IBM Robotic Process Automation 21.0.0 through 21.0.7.latest is vulnerable to unauthorized access to data due to insufficient authorization validation on some API routes. IBM X-Force ID: 245425. **CVE ID : CVE-2023-23476**	https://exchange.xforce.ibmcloud.com/vulnerabilities/245425, https://www.ibm.com/support/pages/node/7017490	A-IBM-ROBO-210823/1068
Vendor: idreamsoft					
Product: icms					
Affected Version(s): 7.0.16					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-2023	9.8	iCMS v7.0.16 was discovered to contain a SQL injection vulnerability via the where parameter at admincp.php. **CVE ID : CVE-2023-39805**	N/A	A-IDR-ICMS-210823/1069
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-2023	9.8	iCMS v7.0.16 was discovered to contain a SQL injection vulnerability via the bakupdata function. **CVE ID : CVE-2023-39806**	N/A	A-IDR-ICMS-210823/1070
Vendor: ikus-soft					
Product: rdiffweb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.8.0					
Allocation of Resources Without Limits or Throttling	03-Aug-2023	6.5	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.8.0. **CVE ID : CVE-2023-4138**	https://github.com/ikus060/rdiffweb/commit/feef0d7b11d86aed29bf98c21526088117964d85	A-IKU-RDIF-210823/1071
Vendor: Imagemagick					
Product: imagemagick					
Affected Version(s): * Up to (excluding) 6.9.12-91					
Missing Release of Memory after Effective Lifetime	08-Aug-2023	7.5	ImageMagick before 6.9.12-91 allows attackers to cause a denial of service (memory consumption) in Magick::Draw. **CVE ID : CVE-2023-39978**	https://github.com/rmagick/rmagick/pull/1406/files, https://github.com/ImageMagick/ImageMagick6/commit/c90e79b3b22fec309cab55af2ee606f71b027b12	A-IMA-IMAG-210823/1072
Vendor: instantcms					
Product: instantcms					
Affected Version(s): * Up to (excluding) 2.16.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2023	9.1	SQL Injection in GitHub repository instantsoft/icms2 prior to 2.16.1-git. **CVE ID : CVE-2023-4188**	https://huntr.dev/bounties/fe9809b6-40ad-4e81-9197-a9aa42e8a7bf, https://github.com/instantsoft/icms2/commit/1dbc3e6c8fbf5d2dc551cb27fad0de3584dee40f	A-INS-INST-210823/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository instantsoft/icms2 prior to 2.16.1-git. **CVE ID : CVE-2023-4187**	https://huntr.dev/bounties/14941381-b669-4756-94fc-cce172472f8b, https://github.com/instantsoft/icms2/commit/1dbc3e6c8fbf5d2dc551cb27fad0de3584dee40f	A-INS-INST-210823/1074
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository instantsoft/icms2 prior to 2.16.1-git. **CVE ID : CVE-2023-4189**	https://huntr.dev/bounties/b00e6986-64e7-464e-ba44-e42476bfcdc4, https://github.com/instantsoft/icms2/commit/1dbc3e6c8fbf5d2dc551cb27fad0de3584dee40f	A-INS-INST-210823/1075
Vendor: Insyde					
Product: insydecrpkg					
Affected Version(s): * Up to (excluding) 01.01.04.0016					
Out-of-bounds Read	03-Aug-2023	7.1	An issue was discovered in InsydeH2O. A malicious operating system can tamper with a runtime-writable EFI variable, leading to out-of-bounds memory reads and a denial of service.	https://www.insyde.com/security-pledge/SA-2023028	A-INS-INSY-210823/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is fixed in version 01.01.04.0016. **CVE ID : CVE-2023-25600**		
Product: insydeh2o					
Affected Version(s): 5.0					
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1077
Affected Version(s): 5.1					
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1078
Affected Version(s): 5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1079
Affected Version(s): 5.3					
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1080
Affected Version(s): 5.4					
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**		
Affected Version(s): 5.5					
Improper Input Validation	07-Aug-2023	5.5	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM. **CVE ID : CVE-2023-27373**	https://www.insyde.com/security-pledge/SA-2023035	A-INS-INSY-210823/1082
Vendor: inventory_management_system_project					
Product: inventory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. This affects an unknown part of the file edit_sell.php. The manipulation of the argument up_pid leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-236217 was	N/A	A-INV-INVE-210823/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-4182**		
Improper Access Control	06-Aug-2023	9.8	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file edit_update.php of the component Password Handler. The manipulation of the argument user_id leads to improper access controls. The attack can be initiated remotely. VDB-236218 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-4183**	N/A	A-INV-INVE-210823/1084
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2023	9.8	A vulnerability was found in SourceCodester Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file sell_return.php. The manipulation of the argument pid leads to sql injection. The attack may be initiated remotely.	N/A	A-INV-INVE-210823/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The associated identifier of this vulnerability is VDB-236219. **CVE ID : CVE-2023-4184**		
Vendor: iscute					
Product: cute_http_file_server					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability, which was classified as problematic, was found in Cute Http File Server 2.0. This affects an unknown part of the component Search. 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-235965 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4118**	N/A	A-ISC-CUTE-210823/1086
Vendor: ivanti					
Product: avalanche					
Affected Version(s): * Up to (excluding) 6.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	10-Aug-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to achieve a remove code execution. Fixed in version 6.4.1. **CVE ID : CVE-2023-32562**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US	A-IVA-AVAL-210823/1087
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2023	9.8	An unauthenticated attacker could achieve the code execution through a RemoteControl server. **CVE ID : CVE-2023-32563**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US	A-IVA-AVAL-210823/1088
Unrestricted Upload of File with Dangerous Type	10-Aug-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution. **CVE ID : CVE-2023-32564**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US	A-IVA-AVAL-210823/1089
Improper Restriction of XML External Entity Reference	10-Aug-2023	9.8	Ivanti Avalanche decodeToMap XML External Entity Processing. Fixed in version 6.4.1. **CVE ID : CVE-2023-32567**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-	A-IVA-AVAL-210823/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				1?language=en_US	
N/A	10-Aug-2023	9.1	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1. **CVE ID : CVE-2023-32565**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US	A-IVA-AVAL-210823/1091
N/A	10-Aug-2023	9.1	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1. **CVE ID : CVE-2023-32566**	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US	A-IVA-AVAL-210823/1092
Product: desktop_\&_server_management					
Affected Version(s): * Up to (excluding) 2022.2					
N/A	10-Aug-2023	7.8	Desktop & Server Management (DSM) may have a possible execution of arbitrary commands. **CVE ID : CVE-2023-28129**	https://forums.ivanti.com/s/article/SA-2023-07-26-CVE-2023-28129	A-IVA-DESK-210823/1093
Affected Version(s): 2022.2					
N/A	10-Aug-2023	7.8	Desktop & Server Management (DSM) may have a possible execution of arbitrary commands.	https://forums.ivanti.com/s/article/SA-2023-07-26-CVE-2023-28129	A-IVA-DESK-210823/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28129		
Product: endpoint_manager_mobile					
Affected Version(s): From (including) 11.10.0 Up to (excluding) 11.10.0.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.2	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to write arbitrary files onto the appliance. **CVE ID : CVE-2023-35081**	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US	A-IVA-ENDP-210823/1095
Affected Version(s): From (including) 11.8.0 Up to (excluding) 11.8.1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.2	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to write arbitrary files onto the appliance. **CVE ID : CVE-2023-35081**	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US	A-IVA-ENDP-210823/1096
Affected Version(s): From (including) 11.9.0 Up to (excluding) 11.9.1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.2	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US	A-IVA-ENDP-210823/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write arbitrary files onto the appliance. **CVE ID : CVE-2023-35081**		
Vendor: jeesite					
Product: jeesite					
Affected Version(s): 1.2.6					
Incorrect Permission Assignment for Critical Resource	04-Aug-2023	5.4	An issue in the delete function in the ActModelController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete models created by the Administrator. **CVE ID : CVE-2023-38991**	N/A	A-JEE-JEES-210823/1098
N/A	02-Aug-2023	4.3	An issue in the delete function in the MenuController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete menus created by the Administrator. **CVE ID : CVE-2023-38990**	https://github.com/thinkgem/jeesite/issues/519	A-JEE-JEES-210823/1099
Vendor: jizhicms					
Product: jizhicms					
Affected Version(s): 1.9.5					
Files or Directories Accessible to External Parties	03-Aug-2023	7.2	An arbitrary file download vulnerability in the /c/PluginsController.php component of jizhi CMS 1.9.5 allows attackers to execute arbitrary	N/A	A-JIZ-JIZH-210823/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via downloading a crafted plugin. **CVE ID : CVE-2023-38948**		
Vendor: Joedolson					
Product: my_content_management					
Affected Version(s): * Up to (including) 1.7.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joseph C Dolson My Content Management plugin <= 1.7.6 versions. **CVE ID : CVE-2023-34377**	N/A	A-JOE-MY_C-210823/1101
Vendor: johnkolbert					
Product: absolute_privacy					
Affected Version(s): * Up to (including) 2.1					
Cross-Site Request Forgery (CSRF)	10-Aug-2023	8.8	The Absolute Privacy plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.1. This is due to missing nonce validation on the 'abpr_profileShortcode' function. This makes it possible for unauthenticated attackers to change user email and password via a forged request granted they can trick a site administrator into	https://plugins.trac.wordpress.org/browser/absolute-privacy/trunk/profile_page.php	A-JOH-ABSO-210823/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID : CVE-2023-4276**		
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')	08-Aug-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-jms/deductScores.php. **CVE ID : CVE-2023-37682**	N/A	A-JUD-JUDG-210823/1103
Vendor: keegnotrub					
Product: art_direction					
Affected Version(s): * Up to (including) 0.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Noël Jackson Art Direction plugin <= 0.2.4 versions. **CVE ID : CVE-2023-37983**	N/A	A-KEE-ART_-210823/1104
Vendor: keyfactor					
Product: ejbca					
Affected Version(s): * Up to (excluding) 8.0.0					
Improper Authentication	03-Aug-2023	8.2	In the Keyfactor EJBCA before 8.0.0, the RA web certificate	https://support.keyfactor.com/hc/en-us/articles/16	A-KEY-EJBC-210823/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			distribution servlet /ejbca/ra/cert allows partial denial of service due to an authentication issue. In configurations using OAuth, disclosure of CA certificates (attributes and public keys) to unauthenticated or less privileged users may occur. **CVE ID : CVE-2023-34196**	671824556827-EJBCA-Security-Advisory-Partial-denial-of-service-attack-on-certificate-distribution-servlet-ejbca-ra-cert	
Vendor: kunduz					
Product: kunduz					
Affected Version(s): * Up to (excluding) 6.2.3					
Use of Hard-coded Cryptographic Key	09-Aug-2023	9.8	Use of Hard-coded Cryptographic Key vulnerability in Sifir Bes Education and Informatics Kunduz - Homework Helper App allows Authentication Abuse, Authentication Bypass.This issue affects Kunduz - Homework Helper App: before 6.2.3. **CVE ID : CVE-2023-3632**	N/A	A-KUN-KUND-210823/1106
Vendor: langchain					
Product: langchain					
Affected Version(s): 0.0.194					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	05-Aug-2023	9.8	An issue in Harrison Chase langchain v.0.0.194 allows an attacker to execute arbitrary code via the python exec calls in the PALChain, affected functions include from_math_prompt and from_colored_object_prompt. **CVE ID : CVE-2023-36095**	https://github.com/langchain-ai/langchain/issues/5872	A-LAN-LANG-210823/1107
Vendor: lavalite					
Product: lavalite					
Affected Version(s): 9.0.0					
N/A	01-Aug-2023	7.5	LavaLite CMS v 9.0.0 is vulnerable to Sensitive Data Exposure. **CVE ID : CVE-2023-36983**	N/A	A-LAV-LAVA-210823/1108
N/A	01-Aug-2023	7.5	LavaLite CMS v 9.0.0 is vulnerable to Sensitive Data Exposure. **CVE ID : CVE-2023-36984**	N/A	A-LAV-LAVA-210823/1109
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): * Up to (excluding) 2.6.0					
Improper Neutralization of Special Elements used in an OS	01-Aug-2023	7.8	OS Command Injection in GitHub repository mlflow/mlflow prior to 2.6.0.	https://github.com/mlflow/mlflow/commit/6dde93758d42455cb90ef324407919ed67668b9b	A-LFP-MLFL-210823/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			**CVE ID : CVE-2023-4033**		
Vendor: libp2p					
Product: go-libp2p					
Affected Version(s): * Up to (excluding) 0.27.8					
Allocation of Resources Without Limits or Throttling	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or	https://github.com/libp2p/go-libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/go-libp2p/security/advisories/GHSA-876p-8259-xjgg	A-LIB-GO-L-210823/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.19.12. There are no known workarounds for this issue. **CVE ID : CVE-2023-39533**		
Affected Version(s): 0.29.0					
Allocation of Resources Without Limits or Throttling	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no	https://github.com/libp2p/go-libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/go-libp2p/security/advisories/GHSA-876p-8259-xjgg	A-LIB-GO-L-210823/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2023-39533**		
Affected Version(s): From (including) 0.28.0 Up to (excluding) 0.28.2					
Allocation of Resources Without Limits or Throttling	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no	https://github.com/libp2p/go-libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/go-libp2p/security/advisories/GHSA-876p-8259-xjgg	A-LIB-GO-L-210823/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2023-39533**		
Vendor: Liferay					
Product: digital_experience_platform					
Affected Version(s): 7.4					
Missing Authorization	02-Aug-2023	4.3	The organization selector in Liferay Portal 7.4.3.81 through 7.4.3.85, and Liferay DXP 7.4 update 81 through 85 does not check user permission, which allows remote authenticated users to obtain a list of all organizations. **CVE ID : CVE-2023-3426**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-3426	A-LIF-DIGI-210823/1114
Product: liferay_portal					
Affected Version(s): From (including) 7.4.3.81 Up to (including) 7.4.3.85					
Missing Authorization	02-Aug-2023	4.3	The organization selector in Liferay Portal 7.4.3.81 through 7.4.3.85, and Liferay DXP 7.4 update 81 through 85 does not check user permission, which allows remote authenticated users to obtain a list of all organizations. **CVE ID : CVE-2023-3426**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-3426	A-LIF-LIFE-210823/1115
Vendor: Linuxfoundation					
Product: yocto					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.6					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1116
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1117
Affected Version(s): 3.3					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	A-LIN-YOCT-210823/1118

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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1119
Affected Version(s): 4.0					
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1121
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1123
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1124
Concurrent Execution using Shared Resource with Improper	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	A-LIN-YOCT-210823/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**		
Vendor: lost_and_found_information_system_project					
Product: lost_and_found_information_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2023	6.1	Cross Site Scripting (XSS) vulnerability in sourcecodester Lost and Found Information System 1.0 allows remote attackers to run arbitrary code via the First Name, Middle Name and Last Name fields on the Create User page. **CVE ID : CVE-2023-36159**	N/A	A-LOS-LOST-210823/1126
Vendor: lw-systems					
Product: benno_mailarchiv					
Affected Version(s): * Up to (excluding) 2.10.2					
Cross-Site Request Forgery (CSRF)	09-Aug-2023	8.8	A CSRF issue was discovered in LWsystems Benno MailArchiv 2.10.1. **CVE ID : CVE-2023-38348**	https://wiki.benno-mailarchiv.de/doku.php	A-LW--BENN-210823/1127
Improper Neutralization of Input	09-Aug-2023	6.1	An issue was discovered in LWsystems Benno MailArchiv 2.10.1.	https://wiki.benno-mailarchiv.de/doku.php	A-LW--BENN-210823/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Attackers can cause XSS via JavaScript content to a mailbox. **CVE ID : CVE-2023-38347**		
Vendor: mage-people					
Product: bus_ticket_booking_with_seat_reservation					
Affected Version(s): * Up to (including) 5.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	The Bus Ticket Booking with Seat Reservation plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab_date' and 'tab_date_r' parameters in versions up to, and including, 5.2.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-4067**	https://www.wordfence.com/threat-intel/vulnerabilities/id/ff2855cb-e4a8-4412-af24-4cee03ae2d43?source=cve	A-MAG-BUS_-210823/1129
Vendor: Matrix					
Product: matrix-appservice-bridge					
Affected Version(s): 9.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Aug-2023	6.5	matrix-appservice-bridge provides an API for setting up bridges. Starting in version 4.0.0 and prior to versions 8.1.2 and 9.0.1, a malicious Matrix server can use a foreign user's MXID in an OpenID exchange, allowing a bad actor to impersonate users when using the provisioning API. The library does not check that the servername part of the `sub` parameter (containing the user's *claimed* MXID) is the the same as the servername we are talking to. A malicious actor could spin up a server on any given domain, respond with a `sub` parameter according to the user they want to act as and use the resulting token to perform provisioning requests. Versions 8.1.2 and 9.0.1 contain a patch. As a workaround, disable the provisioning API. **CVE ID : CVE-2023-38691**	https://github.com/matrix-org/matrix-appservice-bridge/commit/4c6723a5e7beda65cdf1ae5dbb882e8beaac8552	A-MAT-MATR-210823/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0.0 Up to (excluding) 8.1.2					
Improper Authentication	04-Aug-2023	6.5	matrix-appservice-bridge provides an API for setting up bridges. Starting in version 4.0.0 and prior to versions 8.1.2 and 9.0.1, a malicious Matrix server can use a foreign user's MXID in an OpenID exchange, allowing a bad actor to impersonate users when using the provisioning API. The library does not check that the servername part of the `sub` parameter (containing the user's *claimed* MXID) is the the same as the servername we are talking to. A malicious actor could spin up a server on any given domain, respond with a `sub` parameter according to the user they want to act as and use the resulting token to perform provisioning requests. Versions 8.1.2 and 9.0.1 contain a patch. As a workaround, disable the provisioning API.	https://github.com/matrix-org/matrix-appservice-bridge/commit/4c6723a5e7beda65cdf1ae5dbb882e8beaac8552	A-MAT-MATR-210823/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38691		
Product: matrix_irc_bridge					
Affected Version(s): * Up to (excluding) 1.0.1					
Improper Input Validation	04-Aug-2023	9.8	matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it is possible to craft a command with newlines which would not be properly parsed. This would mean you could pass a string of commands as a channel name, which would then be run by the IRC bridge bot. Versions 1.0.1 and above are patched. There are no robust workarounds to the bug. One may disable dynamic channels in the config to disable the most common execution method but others may exist. **CVE ID : CVE-2023-38690**	https://github.com/matrix-org/matrix-appservice-irc/commit/0afb064635d37e039067b5b3d6423448b93026d3	A-MAT-MATR-210823/1132
N/A	04-Aug-2023	3.7	matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it was possible to craft an event such that it would leak part of a targeted message event from another bridged	https://github.com/matrix-org/matrix-appservice-irc/commit/8bbd2b69a16cbcbeffdd9b5c973fd89d61498d75, https://github	A-MAT-MATR-210823/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			room. This required knowing an event ID to target. Version 1.0.1n fixes this issue. As a workaround, set the `matrixHandler.eventCacheSize` config value to `0`. This workaround may impact performance. **CVE ID : CVE-2023-38700**	.com/matrix-org/matrix-appservice-irc/security/advisories/GHSA-c7hh-3v6c-fj4q	
Product: sydent					
Affected Version(s): * Up to (excluding) 2.5.6					
Improper Certificate Validation	04-Aug-2023	5.3	Sydent is an identity server for the Matrix communications protocol. Prior to version 2.5.6, if configured to send emails using TLS, Sydent does not verify SMTP servers' certificates. This makes Sydent's emails vulnerable to interception via a man-in-the-middle (MITM) attack. Attackers with privileged access to the network can intercept room invitations and address confirmation emails. This is patched in Sydent 2.5.6. When patching, make sure that Sydent trusts the certificate of the server it is	https://github.com/matrix-org/sydent/commit/1cd748307c6b168b66154e6c4db715d4b9551261, https://github.com/matrix-org/sydent/security/advisories/GHSA-p6hw-wm59-3g5g, https://github.com/matrix-org/sydent/pull/574	A-MAT-SYDE-210823/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connecting to. This should happen automatically when using properly issued certificates. Those who use self-signed certificates should make sure to copy their Certification Authority certificate, or their self signed certificate if using only one, to the trust store of your operating system. As a workaround, one can ensure Sydent's emails fail to send by setting the configured SMTP server to a loopback or non-routable address under one's control which does not have a listening SMTP server. **CVE ID : CVE-2023-38686**		
Vendor: mattermost					
Product: mattermost					
Affected Version(s): From (including) 7.10.0 Up to (excluding) 7.10.4					
Insertion of Sensitive Information into Log File	11-Aug-2023	7.5	Mattermost fails to sanitize post metadata during audit logging resulting in permalinks contents being logged **CVE ID : CVE-2023-4108**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Aug-2023	6.5	Mattermost fails to check if the requesting user is a guest before performing different actions to public playbooks, resulting a guest being able to view, join, edit, export and archive public playbooks. **CVE ID : CVE-2023-4106**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1136
Incorrect Authorization	11-Aug-2023	6.5	Mattermost fails to properly validate the requesting user permissions when updating a system admin, allowing a user manager to update a system admin's details such as email, first name and last name. **CVE ID : CVE-2023-4107**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1137
Missing Authorization	11-Aug-2023	4.3	Mattermost fails to delete the attachments when deleting a message in a thread allowing a simple user to still be able to access and download the attachment of a deleted message **CVE ID : CVE-2023-4105**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.8.0 Up to (excluding) 7.8.8					
Insertion of Sensitive Information into Log File	11-Aug-2023	7.5	Mattermost fails to sanitize post metadata during audit logging resulting in permalinks contents being logged **CVE ID : CVE-2023-4108**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1139
Missing Authorization	11-Aug-2023	6.5	Mattermost fails to check if the requesting user is a guest before performing different actions to public playbooks, resulting a guest being able to view, join, edit, export and archive public playbooks. **CVE ID : CVE-2023-4106**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1140
Incorrect Authorization	11-Aug-2023	6.5	Mattermost fails to properly validate the requesting user permissions when updating a system admin, allowing a user manager to update a system admin's details such as email, first name and last name. **CVE ID : CVE-2023-4107**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	11-Aug-2023	4.3	Mattermost fails to delete the attachments when deleting a message in a thread allowing a simple user to still be able to access and download the attachment of a deleted message **CVE ID : CVE-2023-4105**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1142
Affected Version(s): From (including) 7.9.0 Up to (excluding) 7.9.6					
Insertion of Sensitive Information into Log File	11-Aug-2023	7.5	Mattermost fails to sanitize post metadata during audit logging resulting in permalinks contents being logged **CVE ID : CVE-2023-4108**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1143
Missing Authorization	11-Aug-2023	6.5	Mattermost fails to check if the requesting user is a guest before performing different actions to public playbooks, resulting a guest being able to view, join, edit, export and archive public playbooks. **CVE ID : CVE-2023-4106**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	11-Aug-2023	6.5	Mattermost fails to properly validate the requesting user permissions when updating a system admin, allowing a user manager to update a system admin's details such as email, first name and last name. **CVE ID : CVE-2023-4107**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1145
Missing Authorization	11-Aug-2023	4.3	Mattermost fails to delete the attachments when deleting a message in a thread allowing a simple user to still be able to access and download the attachment of a deleted message **CVE ID : CVE-2023-4105**	https://mattermost.com/security-updates	A-MAT-MATT-210823/1146
Vendor: mayanets					
Product: e-commerce					
Affected Version(s): * Up to (excluding) 1.1					
Improper Neutralization of Special Elements used in an SQL Command	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mAyaNet E-	N/A	A-MAY-E-CO-210823/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Commerce Software allows SQL Injection.This issue affects E-Commerce Software: before 1.1. **CVE ID : CVE-2023-3898**		
Vendor: mayurik					
Product: free_hospital_management_system_for_small_practices					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected is an unknown function of the file /vm/doctor/doctors.php?action=view. 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. VDB-236214 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-4179**	N/A	A-MAY-FREE-210823/1148
Improper Neutralization of Special Elements used in an	06-Aug-2023	9.8	A vulnerability classified as critical was found in SourceCodester Free Hospital Management System	N/A	A-MAY-FREE-210823/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			for Small Practices 1.0. Affected by this vulnerability is an unknown functionality of the file /vm/login.php. The manipulation of the argument useremail/userpass word 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-236215. **CVE ID : CVE-2023-4180**		
Improper Enforcement of Behavioral Workflow	06-Aug-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected by this issue is some unknown functionality of the file /vm/admin/delete-doctor.php?id=2 of the component Redirect Handler. The manipulation leads to enforcement of behavioral workflow. The attack may be launched	N/A	A-MAY-FREE-210823/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-236216. **CVE ID : CVE-2023-4181**		
Product: inventory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file product_data.php.. The manipulation of the argument columns[1][data] leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-236290 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-4200**	N/A	A-MAY-INVE-210823/1151
Improper Neutralization of Special Elements	07-Aug-2023	9.8	A vulnerability was found in SourceCodester Inventory Management System	N/A	A-MAY-INVE-210823/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			1.0 and classified as critical. This issue affects some unknown processing of the file ex_catagory_data.php. The manipulation of the argument columns[1][data] 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-236291. **CVE ID : CVE-2023-4201**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	7.5	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. This affects an unknown part of the file catagory_data.php. The manipulation of the argument columns[1][data] 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-236289 was	N/A	A-MAY-INVE-210823/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-4199**		
Product: online_hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2023	9.8	A vulnerability was found in SourceCodester Online Hospital Management System 1.0. It has been classified as critical. Affected is an unknown function of the file patientlogin.php. The manipulation of the argument loginid/password 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-236220. **CVE ID : CVE-2023-4185**	N/A	A-MAY-ONLI-210823/1154
Vendor: mediatek					
Product: iot_yocto					
Affected Version(s): 23.0					
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	A-MED-IOT_-210823/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
Vendor: metabase					
Product: metabase					
Affected Version(s): * Up to (excluding) 0.43.7.3					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database.	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): * Up to (excluding) 1.43.7.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): From (including) 0.44.0 Up to (excluding) 0.44.7.3					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): From (including) 0.45.0 Up to (excluding) 0.45.4.3					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code.	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): From (including) 0.46.0 Up to (excluding) 0.46.6.4					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4,	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): From (including) 1.44.0 Up to (excluding) 1.44.7.3					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37470		
Affected Version(s): From (including) 1.45.0 Up to (excluding) 1.45.4.3					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Affected Version(s): From (including) 1.46.0 Up to (excluding) 1.46.6.4					
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	9.8	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code	https://github.com/metabase/metabase/security/advisories/GHSA-p7w3-9m58-rq83	A-MET-META-210823/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite. **CVE ID : CVE-2023-37470**		
Vendor: metersphere					
Product: metersphere					
Affected Version(s): * Up to (excluding) 2.10.4					
Missing Authorization	04-Aug-2023	7.5	MeterSphere is an open-source continuous testing platform. Prior to version 2.10.4 LTS, some interfaces of the Cloud version of MeterSphere do not have configuration permissions, and are sensitively leaked by attackers. Version 2.10.4 LTS contains a patch for this issue. **CVE ID : CVE-2023-38494**	https://github.com/metersphere/metersphere/commit/a23f75d93b666901fd148d834df9384f6f24cf28	A-MET-METE-210823/1164
Vendor: mi					
Product: xiaomi_cloud					
Affected Version(s): * Up to (including) 1.12.0.0.25					
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	6.1	A XSS vulnerability exists in the Xiaomi cloud service Application product. The vulnerability is caused by Webview's whitelist checking	https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=322	A-MI-XIAO-210823/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			function allowing javascript protocol to be loaded and can be exploited by attackers to steal Xiaomi cloud service account's cookies. **CVE ID : CVE-2023-26316**		
Vendor: Microsoft					
Product: .net					
Affected Version(s): 2.0					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1166
Affected Version(s): 6.0.0					
N/A	08-Aug-2023	7.5	.NET Core and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38178	A-MIC-.NET-210823/1167
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-.NET-210823/1168
Affected Version(s): 7.0.0					
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-.NET-210823/1169
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35390**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35390	A-MIC-.NET-210823/1170
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.21					
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability **CVE ID : CVE-2023-35391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-.NET-210823/1171
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.10					
N/A	08-Aug-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35390**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35390	A-MIC-.NET-210823/1172
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.10					
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability **CVE ID : CVE-2023-35391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-.NET-210823/1173
Product: .net_framework					
Affected Version(s): 3.5					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1175
Affected Version(s): 4.6.2					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1176
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1177
Affected Version(s): 4.7					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1178
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1179
Affected Version(s): 4.7.1					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1181
Affected Version(s): 4.7.2					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1182
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1183
Affected Version(s): 4.8					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1184
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1185
Affected Version(s): 4.8.1					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	A-MIC-.NET-210823/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	A-MIC-.NET-210823/1187
Product: 365_apps					
Affected Version(s): -					
N/A	08-Aug-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-35371**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371	A-MIC-365_-210823/1188
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35372**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35372	A-MIC-365_-210823/1189
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-36865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36865	A-MIC-365_-210823/1190
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-36866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36866	A-MIC-365_-210823/1191
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-36895**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895	A-MIC-365_-210823/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-365_-210823/1193
N/A	08-Aug-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-36893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36893	A-MIC-365_-210823/1194
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-365_-210823/1195
Product: asp.net_core					
Affected Version(s): 2.1					
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability **CVE ID : CVE-2023-35391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-ASP.-210823/1196
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-ASP.-210823/1197
Product: azure_arc-enabled_servers					
Affected Version(s): * Up to (excluding) 1.33.02399.0					
N/A	08-Aug-2023	7	Azure Arc-Enabled Servers Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-AZUR-210823/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38176	bility/CVE-2023-38176	
Product: azure_hdinsights					
Affected Version(s): -					
N/A	08-Aug-2023	4.6	Azure HDInsight Jupyter Notebook Spoofing Vulnerability **CVE ID : CVE-2023-35394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35394	A-MIC-AZUR-210823/1199
N/A	08-Aug-2023	4.5	Azure Apache Hive Spoofing Vulnerability **CVE ID : CVE-2023-35393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35393	A-MIC-AZUR-210823/1200
N/A	08-Aug-2023	4.5	Azure Apache Oozie Spoofing Vulnerability **CVE ID : CVE-2023-36877**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36877	A-MIC-AZUR-210823/1201
N/A	08-Aug-2023	4.5	Azure Apache Ambari Spoofing Vulnerability **CVE ID : CVE-2023-36881**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36881	A-MIC-AZUR-210823/1202
N/A	08-Aug-2023	4.5	Azure Apache Hadoop Spoofing Vulnerability **CVE ID : CVE-2023-38188**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38188	A-MIC-AZUR-210823/1203
Product: dynamics_365					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.47.08					
N/A	08-Aug-2023	6.5	Microsoft Dynamics 365 On-Premises Remote Code	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-DYNA-210823/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35389**	bility/CVE-2023-35389	
Affected Version(s): From (including) 9.1 Up to (excluding) 9.1.18.22					
N/A	08-Aug-2023	6.5	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability **CVE ID : CVE-2023-35389**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35389	A-MIC-DYNA-210823/1205
Product: dynamics_365_business_central					
Affected Version(s): 2023					
N/A	08-Aug-2023	7.2	Microsoft Dynamics Business Central Elevation Of Privilege Vulnerability **CVE ID : CVE-2023-38167**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38167	A-MIC-DYNA-210823/1206
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 115.0.1901.200					
N/A	07-Aug-2023	6.5	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability **CVE ID : CVE-2023-38157**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38157	A-MIC-EDGE-210823/1207
Product: exchange_server					
Affected Version(s): 2016					
Improper Restriction of Excessive Authentication Attempts	08-Aug-2023	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21709**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709	A-MIC-EXCH-210823/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	8.8	Microsoft Exchange Remote Code Execution Vulnerability **CVE ID : CVE-2023-35368**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368	A-MIC-EXCH-210823/1209
N/A	08-Aug-2023	8.8	Microsoft Exchange Server Spoofing Vulnerability **CVE ID : CVE-2023-38181**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181	A-MIC-EXCH-210823/1210
N/A	08-Aug-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185	A-MIC-EXCH-210823/1211
N/A	08-Aug-2023	8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388	A-MIC-EXCH-210823/1212
N/A	08-Aug-2023	8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-38182**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182	A-MIC-EXCH-210823/1213
Affected Version(s): 2019					
Improper Restriction of Excessive Authentication Attempts	08-Aug-2023	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability **CVE ID : CVE-2023-21709**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709	A-MIC-EXCH-210823/1214
N/A	08-Aug-2023	8.8	Microsoft Exchange Remote Code	https://msrc.microsoft.com	A-MIC-EXCH-210823/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-35368**	/update-guide/vulnerability/CVE-2023-35368	
N/A	08-Aug-2023	8.8	Microsoft Exchange Server Spoofing Vulnerability **CVE ID : CVE-2023-38181**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181	A-MIC-EXCH-210823/1216
N/A	08-Aug-2023	8.8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-38185**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185	A-MIC-EXCH-210823/1217
N/A	08-Aug-2023	8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-35388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388	A-MIC-EXCH-210823/1218
N/A	08-Aug-2023	8	Microsoft Exchange Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-38182**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182	A-MIC-EXCH-210823/1219
Product: hevc_video_extensions					
Affected Version(s): * Up to (excluding) 2.0.61933.0					
N/A	08-Aug-2023	7.8	HEVC Video Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-38170**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38170	A-MIC-HEVC-210823/1220
Product: odbc_driver_for_sql_server					
Affected Version(s): 17.0.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-ODBC-210823/1221
Affected Version(s): 17.10.3.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-ODBC-210823/1222
Affected Version(s): 17.10.4.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-ODBC-210823/1223
Affected Version(s): 18.0.1.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-ODBC-210823/1224
Affected Version(s): 18.1.2.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-ODBC-210823/1225
Affected Version(s): 18.2.1.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-ODBC-210823/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-38169**	bility/CVE-2023-38169	
Product: office					
Affected Version(s): 2021					
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-OFFI-210823/1227
Affected Version(s): 2016					
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-36895**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895	A-MIC-OFFI-210823/1228
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-OFFI-210823/1229
Affected Version(s): 2019					
N/A	08-Aug-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-35371**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371	A-MIC-OFFI-210823/1230
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35372**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35372	A-MIC-OFFI-210823/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-36865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36865	A-MIC-OFFI-210823/1232
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-36866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36866	A-MIC-OFFI-210823/1233
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-36895**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895	A-MIC-OFFI-210823/1234
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-OFFI-210823/1235
N/A	08-Aug-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-36893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36893	A-MIC-OFFI-210823/1236
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-OFFI-210823/1237
Affected Version(s): 2013					
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code	https://msrc.microsoft.com/update-	A-MIC-OFFI-210823/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-36895**	guide/vulnerability/CVE-2023-36895	
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-OFFI-210823/1239
Affected Version(s): 2013_rt					
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-36895**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895	A-MIC-OFFI-210823/1240
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-OFFI-210823/1241
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	08-Aug-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-35371**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371	A-MIC-OFFI-210823/1242
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35372**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35372	A-MIC-OFFI-210823/1243
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code	https://msrc.microsoft.com	A-MIC-OFFI-210823/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-36865**	/update-guide/vulnerability/CVE-2023-36865	
N/A	08-Aug-2023	7.8	Microsoft Office Visio Remote Code Execution Vulnerability **CVE ID : CVE-2023-36866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36866	A-MIC-OFFI-210823/1245
N/A	08-Aug-2023	7.8	Microsoft Outlook Remote Code Execution Vulnerability **CVE ID : CVE-2023-36895**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895	A-MIC-OFFI-210823/1246
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-36896**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896	A-MIC-OFFI-210823/1247
N/A	08-Aug-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-36893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36893	A-MIC-OFFI-210823/1248
Product: office_online_server					
Affected Version(s): -					
N/A	08-Aug-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-35371**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371	A-MIC-OFFI-210823/1249
N/A	08-Aug-2023	7.8	Microsoft Excel Remote Code	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-OFFI-210823/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-36896**	bility/CVE-2023-36896	
Product: ole_db_driver_for_sql_server					
Affected Version(s): 18.0.2					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1251
Affected Version(s): 18.1.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1252
Affected Version(s): 18.2.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1253
Affected Version(s): 18.2.2					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1254
Affected Version(s): 18.2.3					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-OLE_-210823/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38169	bility/CVE-2023-38169	
Affected Version(s): 18.3.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1256
Affected Version(s): 18.4.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1257
Affected Version(s): 18.5.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1258
Affected Version(s): 18.6.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1259
Affected Version(s): 19.0.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1260
Affected Version(s): 19.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1261
Affected Version(s): 19.2.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1262
Affected Version(s): 19.3.0					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1263
Affected Version(s): 19.3.1					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-OLE_-210823/1264
Product: outlook					
Affected Version(s): 2016					
N/A	08-Aug-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-36893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36893	A-MIC-OUTL-210823/1265
Affected Version(s): 2013					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Microsoft Outlook Spoofing Vulnerability **CVE ID : CVE-2023-36893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36893	A-MIC-OUTL-210823/1266
Product: sharepoint_server					
Affected Version(s): -					
N/A	08-Aug-2023	8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-36891**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36891	A-MIC-SHAR-210823/1267
N/A	08-Aug-2023	8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-36892**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36892	A-MIC-SHAR-210823/1268
N/A	08-Aug-2023	6.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2023-36890**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36890	A-MIC-SHAR-210823/1269
N/A	08-Aug-2023	6.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2023-36894**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36894	A-MIC-SHAR-210823/1270
Affected Version(s): 2016					
N/A	08-Aug-2023	6.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2023-36894**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36894	A-MIC-SHAR-210823/1271
Affected Version(s): 2019					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-36891**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36891	A-MIC-SHAR-210823/1272
N/A	08-Aug-2023	8	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-36892**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36892	A-MIC-SHAR-210823/1273
N/A	08-Aug-2023	6.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2023-36890**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36890	A-MIC-SHAR-210823/1274
N/A	08-Aug-2023	6.5	Microsoft SharePoint Server Information Disclosure Vulnerability **CVE ID : CVE-2023-36894**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36894	A-MIC-SHAR-210823/1275
Product: sql_server					
Affected Version(s): 2022					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-SQL_-210823/1276
Affected Version(s): 2019					
N/A	08-Aug-2023	8.8	Microsoft OLE DB Remote Code Execution Vulnerability **CVE ID : CVE-2023-38169**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38169	A-MIC-SQL_-210823/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: teams					
Affected Version(s): * Up to (excluding) 1.0.0.2023070204					
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328	A-MIC-TEAM-210823/1278
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330	A-MIC-TEAM-210823/1279
Affected Version(s): * Up to (excluding) 1.6.00.17554					
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328	A-MIC-TEAM-210823/1280
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330	A-MIC-TEAM-210823/1281
Affected Version(s): * Up to (excluding) 1.6.00.18681					
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328	A-MIC-TEAM-210823/1282
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-TEAM-210823/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29330	bility/CVE-2023-29330	
Affected Version(s): * Up to (excluding) 5.12.1					
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29328**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328	A-MIC-TEAM-210823/1284
N/A	08-Aug-2023	8.8	Microsoft Teams Remote Code Execution Vulnerability **CVE ID : CVE-2023-29330**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330	A-MIC-TEAM-210823/1285
Product: visual_studio_2010_tools_for_office_runtime					
Affected Version(s): -					
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-VISU-210823/1286
Product: visual_studio_2017					
Affected Version(s): From (including) 15.0 Up to (excluding) 15.9.56					
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-VISU-210823/1287
Product: visual_studio_2019					
Affected Version(s): From (including) 16.0 Up to (excluding) 16.11.29					
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-VISU-210823/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36897	bility/CVE-2023-36897	
Product: visual_studio_2022					
Affected Version(s): From (including) 17.2.0 Up to (excluding) 17.2.18					
N/A	08-Aug-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35390**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35390	A-MIC-VISU-210823/1289
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability **CVE ID : CVE-2023-35391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-VISU-210823/1290
N/A	08-Aug-2023	7.5	.NET Core and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38178	A-MIC-VISU-210823/1291
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-VISU-210823/1292
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-VISU-210823/1293
Affected Version(s): From (including) 17.4.0 Up to (excluding) 17.4.10					
N/A	08-Aug-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	A-MIC-VISU-210823/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35390	bility/CVE-2023-35390	
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability **CVE ID : CVE-2023-35391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-VISU-210823/1295
N/A	08-Aug-2023	7.5	.NET Core and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38178**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38178	A-MIC-VISU-210823/1296
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-VISU-210823/1297
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-VISU-210823/1298
Affected Version(s): From (including) 17.6.0 Up to (excluding) 17.6.6					
N/A	08-Aug-2023	7.8	.NET and Visual Studio Remote Code Execution Vulnerability **CVE ID : CVE-2023-35390**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35390	A-MIC-VISU-210823/1299
N/A	08-Aug-2023	7.5	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35391	A-MIC-VISU-210823/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35391		
N/A	08-Aug-2023	7.5	.NET and Visual Studio Denial of Service Vulnerability **CVE ID : CVE-2023-38180**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180	A-MIC-VISU-210823/1301
N/A	08-Aug-2023	6.5	Visual Studio Tools for Office Runtime Spoofing Vulnerability **CVE ID : CVE-2023-36897**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36897	A-MIC-VISU-210823/1302
Product: windows_defender					
Affected Version(s): * Up to (excluding) 1.1.23060.3001					
N/A	08-Aug-2023	7.8	Microsoft Windows Defender Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38175**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38175	A-MIC-WIND-210823/1303
Vendor: mindsdb					
Product: mindsdb					
Affected Version(s): * Up to (excluding) 23.7.4.0					
Missing Encryption of Sensitive Data	04-Aug-2023	6.5	MindsDB's AI Virtual Database allows developers to connect any AI/ML model to any datasource. Prior to version 23.7.4.0, a call to requests with `verify=False` disables SSL certificate checks. This rule enforces always verifying SSL certificates for methods in the	https://github.com/mindsdb/mindsdb/security/advisories/GHSA-8hx6-qv6f-xgcw, https://github.com/mindsdb/mindsdb/commit/083afcf6567cf51aa7d89ea892fd97689919053b	A-MIN-MIND-210823/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Requests library. In version 23.7.4.0, certificates are validated by default, which is the desired behavior. **CVE ID : CVE-2023-38699**		
Vendor: MIT					
Product: kerberos_5					
Affected Version(s): * Up to (excluding) 1.20.2					
Access of Uninitialized Pointer	07-Aug-2023	6.5	lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count. **CVE ID : CVE-2023-36054**	https://github.com/krb5/krb5/compare/krb5-1.20.1-final...krb5-1.20.2-final, https://github.com/krb5/krb5/commit/ef08b09c9459551aabbe7924fb176f1583053cdd, https://github.com/krb5/krb5/compare/krb5-1.21-final...krb5-1.21.1-final	A-MIT-KERB-210823/1305
Affected Version(s): 1.21					
Access of Uninitialized Pointer	07-Aug-2023	6.5	lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user	https://github.com/krb5/krb5/compare/krb5-1.20.1-final...krb5-1.20.2-final, https://github.com/krb5/krb5/commit/ef	A-MIT-KERB-210823/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count. **CVE ID : CVE-2023-36054**	08b09c9459551aabbe7924fb176f1583053cdd, https://github.com/krb5/krb5/compare/krb5-1.21-final...krb5-1.21.1-final	
Vendor: Mitsubishielectric					
Product: gt_designer3					
Affected Version(s): * Up to (excluding) 1.300n					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	A-MIT-GT_D-210823/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt_softgot2000					
Affected Version(s): * Up to (excluding) 1.300n					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	A-MIT-GT_S-210823/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Mongodb					
Product: ops_manager_server					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.22					
Improper Privilege Management	08-Aug-2023	7.2	In MongoDB Ops Manager v5.0 prior to 5.0.22 and v6.0 prior to 6.0.17 it is possible for an authenticated user with project owner or project user admin access to generate an API key with the privileges of org owner resulting in privilege escalation. **CVE ID : CVE-2023-4009**	https://www.mongodb.com/docs/ops-manager/v5.0/release-notes/application/#onprem-server-5-0-22, https://www.mongodb.com/docs/ops-manager/current/release-notes/application/#onprem-server-6-0	A-MON-OPS_-210823/1309
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.17					
Improper Privilege Management	08-Aug-2023	7.2	In MongoDB Ops Manager v5.0 prior to 5.0.22 and v6.0 prior to 6.0.17 it is possible for an authenticated user with project owner or project user admin access to generate an API key with the privileges of org owner resulting in privilege escalation. **CVE ID : CVE-2023-4009**	https://www.mongodb.com/docs/ops-manager/v5.0/release-notes/application/#onprem-server-5-0-22, https://www.mongodb.com/docs/ops-manager/current/release-notes/application/#onprem-server-6-0	A-MON-OPS_-210823/1310
Vendor: monsterinsights					
Product: exactmetrics					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.14.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ExactMetrics plugin <= 7.14.1 versions. **CVE ID : CVE-2023-23880**	N/A	A-MON-EXAC-210823/1311
Vendor: mooj					
Product: proforms					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection. **CVE ID : CVE-2023-34476**	N/A	A-MOO-PROF-210823/1312
Vendor: moosocial					
Product: moostore					
Affected Version(s): 3.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2023	6.1	A vulnerability, which was classified as problematic, was found in mooSocial mooStore 3.1.6. Affected is an unknown function of the file /search/index. The manipulation of the argument q leads to cross site scripting. It is possible to launch the attack remotely.	N/A	A-MOO-MOOS-210823/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The identifier of this vulnerability is VDB-236208. **CVE ID : CVE-2023-4173**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2023	6.1	A vulnerability has been found in mooSocial mooStore 3.1.6 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. The identifier VDB-236209 was assigned to this vulnerability. **CVE ID : CVE-2023-4174**	N/A	A-MOO-MOOS-210823/1314
Product: mootravel					
Affected Version(s): 3.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2023	6.1	A vulnerability was found in mooSocial mooTravel 3.1.8 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. The attack may be launched remotely. VDB-236210 is the	N/A	A-MOO-MOOT-210823/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. **CVE ID : CVE-2023-4175**		
Vendor: motocms					
Product: motocms					
Affected Version(s): 3.4.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Aug-2023	9.8	MotoCMS Version 3.4.3 Store Category Template was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the keyword parameter. **CVE ID : CVE-2023-36210**	N/A	A-MOT-MOTO-210823/1316
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	9.8	SQL injection vulnerability in MotoCMS v.3.4.3 allows a remote attacker to gain privileges via the keyword parameter of the search function. **CVE ID : CVE-2023-36213**	N/A	A-MOT-MOTO-210823/1317
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 116.0					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.	A-MOZ-FIRE-210823/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, and Thunderbird 115.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1. **CVE ID : CVE-2023-4057**	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1319
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115. Some of these bugs showed evidence of memory	https://www.mozilla.org/security/advisor	A-MOZ-FIRE-210823/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116. **CVE ID : CVE-2023-4058**	ies/mfsa2023-29/	
N/A	01-Aug-2023	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4047**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1321
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2023	7.5	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4050**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1323
N/A	01-Aug-2023	7.5	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 116. **CVE ID : CVE-2023-4051**	https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1324
N/A	01-Aug-2023	7.5	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisor	A-MOZ-FIRE-210823/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4055**	ies/mfsa2023-29/	
Improper Link Resolution Before File Access ('Link Following')	01-Aug-2023	6.5	The Firefox updater created a directory writable by non-privileged users. When uninstalling Firefox, any files in that directory would be recursively deleted with the permissions of the uninstalling user account. This could be combined with creation of a junction (a form of symbolic link) to allow arbitrary file deletion controlled by the non-privileged user. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1. **CVE ID : CVE-2023-4052**	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1326
Improper Link Resolution Before File	01-Aug-2023	6.5	A website could have obscured the full screen notification by using a URL with	https://www.mozilla.org/security/advisor	A-MOZ-FIRE-210823/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 116. **CVE ID : CVE-2023-4053**	ies/mfsa2023-29/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2023	5.9	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4049**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1328
N/A	01-Aug-2023	5.5	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 102.14, Firefox ESR < 115.1,	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/, https://www.	A-MOZ-FIRE-210823/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 102.14, and Thunderbird < 115.1. **CVE ID : CVE-2023-4054**	mozilla.org/security/advisories/mfsa2023-33/	
Origin Validation Error	01-Aug-2023	5.3	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4045**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1330
N/A	01-Aug-2023	5.3	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4046**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1331
Product: firefox_esr					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 115.1					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, and Thunderbird 115.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1. **CVE ID : CVE-2023-4057**	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1332
Improper Link Resolution Before File Access ('Link Following')	01-Aug-2023	6.5	The Firefox updater created a directory writable by non-privileged users. When uninstalling Firefox, any files in that directory would be recursively deleted with the permissions of the uninstalling user account. This could be combined with creation of a junction (a form of symbolic link) to allow arbitrary file deletion controlled by the non-privileged user.	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This bug only affects Firefox on Windows. Other operating systems are unaffected. This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1. **CVE ID : CVE-2023-4052**		
Affected Version(s): From (including) 102.0 Up to (excluding) 102.14					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1334
N/A	01-Aug-2023	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.	A-MOZ-FIRE-210823/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4047**	mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1336
Out-of-bounds Write	01-Aug-2023	7.5	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4050**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Aug-2023	7.5	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4055**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1338
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2023	5.9	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4049**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1339
N/A	01-Aug-2023	5.5	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code.	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisor	A-MOZ-FIRE-210823/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This bug only affects Firefox on Windows. Other operating systems are unaffected. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, Firefox ESR < 115.1, Thunderbird < 102.14, and Thunderbird < 115.1. **CVE ID : CVE-2023-4054**	ies/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/, https://www.mozilla.org/security/advisories/mfsa2023-33/	
Origin Validation Error	01-Aug-2023	5.3	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4045**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1341
N/A	01-Aug-2023	5.3	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisor	A-MOZ-FIRE-210823/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4046**	ies/mfsa2023-29/	
Affected Version(s): From (including) 115.0 Up to (excluding) 115.1					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1343
N/A	01-Aug-2023	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14,	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/se	A-MOZ-FIRE-210823/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 115.1. **CVE ID : CVE-2023-4047**	curity/advisories/mfsa2023-29/	
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1345
Out-of-bounds Write	01-Aug-2023	7.5	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4050**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1346
N/A	01-Aug-2023	7.5	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.	A-MOZ-FIRE-210823/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4055**	mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2023	5.9	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4049**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1348
N/A	01-Aug-2023	5.5	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116,	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023	A-MOZ-FIRE-210823/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 102.14, Firefox ESR < 115.1, Thunderbird < 102.14, and Thunderbird < 115.1. **CVE ID : CVE-2023-4054**	-29/, https://www.mozilla.org/security/advisories/mfsa2023-33/	
Origin Validation Error	01-Aug-2023	5.3	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4045**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1350
N/A	01-Aug-2023	5.3	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4046**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	A-MOZ-FIRE-210823/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: multiparcels					
Product: multiparcels_shipping_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.14.14					
Missing Authorization	07-Aug-2023	8.1	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.14.14 does not have authorisation when deleting shipment, allowing any authenticated users, such as subscriber to delete arbitrary shipment **CVE ID : CVE-2023-3365**	N/A	A-MUL-MULT-210823/1352
Affected Version(s): * Up to (excluding) 1.14.15					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	8.8	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.14.15 does not properly sanitize and escape a parameter before using it in an SQL statement, which could allow any authenticated users, such as subscribers, to perform SQL Injection attacks. **CVE ID : CVE-2023-2843**	N/A	A-MUL-MULT-210823/1353
Affected Version(s): * Up to (excluding) 1.15.4					
Improper Neutralization of Input	07-Aug-2023	6.1	The MultiParcels Shipping For WooCommerce WordPress plugin	N/A	A-MUL-MULT-210823/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			before 1.15.4 does not sanitise and escape various parameters before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-3671**		
Vendor: n-able					
Product: n-central					
Affected Version(s): * Up to (excluding) 2023.4					
N/A	04-Aug-2023	7	An issue found in N-able Technologies N-central Server before 2023.4 allows a local attacker to execute arbitrary code via the monitoring function of the server. **CVE ID : CVE-2023-30297**	N/A	A-N-A-N-CE-210823/1355
Vendor: Netapp					
Product: clustered_data_ontap					
Affected Version(s): 9.0					
Integer Overflow or Wraparound	01-Aug-2023	7.5	A set of carefully crafted ipv6 packets can trigger an integer overflow in the calculation of a fragment reassembled packet's payload length field. This allows an attacker to	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:06.ipv6.asc	A-NET-CLUS-210823/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a kernel panic, resulting in a denial of service. **CVE ID : CVE-2023-3107**		
Vendor: netbox_project					
Product: netbox					
Affected Version(s): 3.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Netbox v3.4.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Link templates. **CVE ID : CVE-2023-37625**	https://github.com/netbox-community/netbox/issues/12205	A-NET-NETB-210823/1357
Vendor: never5					
Product: post_connector					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Never5 Post Connector plugin <= 1.0.9 versions. **CVE ID : CVE-2023-28931**	N/A	A-NEV-POST-210823/1358
Vendor: nexb					
Product: scancode.io					
Affected Version(s): * Up to (excluding) 32.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Aug-2023	8.8	ScanCode.io is a server to script and automate software composition analysis with ScanPipe pipelines. Prior to version 32.5.1, the software has a possible command injection vulnerability in the docker fetch process as it allows to append malicious commands in the `docker_reference` parameter. In the function `scanpipe/pipes/fetch.py:fetch_docker_image` the parameter `docker_reference` is user controllable. The `docker_reference` variable is then passed to the vulnerable function `get_docker_image_platform`. However, the `get_docker_image_platform` function constructs a shell command with the passed `docker_reference`. The `pipes.run_command` then executes the shell command without any prior	https://github.com/nexB/scancode.io/security/advisories/GHSA-2ggp-cmvm-f62f, https://github.com/nexB/scancode.io/commit/07ec0de1964b14bf085a1c9a27ece2b61ab6105c	A-NEX-SCAN-210823/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization, making the function vulnerable to command injections. A malicious user who is able to create or add inputs to a project can inject commands. Although the command injections are blind and the user will not receive direct feedback without logs, it is still possible to cause damage to the server/container. The vulnerability appears for example if a malicious user adds a semicolon after the input of `docker://;`, it would allow appending malicious commands. Version 32.5.1 contains a patch for this issue. The `docker_reference` input should be sanitized to avoid command injections and, as a workaround, one may avoid creating commands with user controlled input directly. **CVE ID : CVE-2023-39523**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: nextgen					
Product: mirth_connect					
Affected Version(s): 4.3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2023	9.8	A remote command execution (RCE) vulnerability in NextGen Mirth Connect v4.3.0 allows attackers to execute arbitrary commands on the hosting server. **CVE ID : CVE-2023-37679**	N/A	A-NEX-MIRT-210823/1360
Vendor: ngiflib_project					
Product: ngiflib					
Affected Version(s): * Up to (excluding) 2023-07-14					
N/A	02-Aug-2023	5.5	ngiflib commit fb271 was discovered to contain a segmentation violation via the function "main" at gif2tag.c. This vulnerability is triggered when running the program gif2tga. **CVE ID : CVE-2023-39113**	https://github.com/miniupnp/ngiflib/issues/27	A-NGI-NGIF-210823/1361
Affected Version(s): * Up to (excluding) 2023-07-21					
N/A	02-Aug-2023	5.5	ngiflib commit 84a75 was discovered to contain a segmentation violation via the function SDL_LoadAnimatedGif at ngiflibSDL.c. This vulnerability is	https://github.com/miniupnp/ngiflib/issues/29	A-NGI-NGIF-210823/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggered when running the program SDLaffgif. **CVE ID : CVE-2023-39114**		
Vendor: Nomachine					
Product: nomachine					
Affected Version(s): * Up to (excluding) 8.8.1					
Improper Link Resolution Before File Access ('Link Following')	04-Aug-2023	9.1	An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-owned files by using hardlinks. **CVE ID : CVE-2023-39107**	https://kb.nomachine.com/TR07U10948	A-NOM-NOMA-210823/1363
Vendor: nozominetworks					
Product: cmc					
Affected Version(s): * Up to (excluding) 22.6.2					
Session Fixation	09-Aug-2023	7	In certain conditions, depending on timing and the usage of the Chrome web browser, Guardian/CMC versions before 22.6.2 do not always completely invalidate the user session upon logout. Thus an authenticated local attacker may gain acces to the original user's session.	https://security.nozominetworks.com/NN-2023:8-01	A-NOZ-CMC-210823/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24477		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2023	6.5	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the sorting parameter, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application. Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way. **CVE ID : CVE-2023-22378**	https://security.nozominetworks.com/NN-2023:2-01	A-NOZ-CMC-210823/1365
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2023	6.5	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the alerts_count component, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS	https://security.nozominetworks.com/NN-2023:3-01	A-NOZ-CMC-210823/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used by the web application. Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way. **CVE ID : CVE-2023-23574**		
Product: guardian					
Affected Version(s): * Up to (excluding) 22.6.2					
Session Fixation	09-Aug-2023	7	In certain conditions, depending on timing and the usage of the Chrome web browser, Guardian/CMC versions before 22.6.2 do not always completely invalidate the user session upon logout. Thus an authenticated local attacker may gain acces to the original user's session. **CVE ID : CVE-2023-24477**	https://security.nozominetworks.com/NN-2023:8-01	A-NOZ-GUAR-210823/1367
Improper Neutralization of Special Elements used in an	09-Aug-2023	6.5	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in	https://security.nozominetworks.com/NN-2023:2-01	A-NOZ-GUAR-210823/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			the sorting parameter, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application. Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way. **CVE ID : CVE-2023-22378**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2023	6.5	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the alerts_count component, allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application. Authenticated users can extract arbitrary information from the DBMS in an uncontrolled way.	https://security.nozominetworks.com/NN-2023:3-01	A-NOZ-GUAR-210823/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23574		
Vendor: nsthemes					
Product: ns_coupon_to_become_customer					
Affected Version(s): * Up to (including) 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NsThemes NS Coupon To Become Customer plugin <= 1.2.2 versions. **CVE ID : CVE-2023-27422**	N/A	A-NST-NS_C-210823/1370
Vendor: Ntpsec					
Product: ntpsec					
Affected Version(s): 1.2.2					
N/A	07-Aug-2023	7.5	ntpd will crash if the server is not NTS-enabled (no certificate) and it receives an NTS-enabled client request (mode 3). **CVE ID : CVE-2023-4012**	https://gitlab.com/NTPsec/ntpsec/-/issues/794	A-NTP-NTPS-210823/1371
Vendor: Nvidia					
Product: omniverse_launcher					
Affected Version(s): * Up to (excluding) 1.8.11					
N/A	03-Aug-2023	5.3	NVIDIA Omniverse Workstation Launcher for Windows and Linux contains a vulnerability in the authentication flow, where a user's access	https://nvidia.custhelp.com/app/answers/detail/a_id/5472	A-NVI-OMNI-210823/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			token is displayed in the browser user's address bar. An attacker could use this token to impersonate the user to access launcher resources. A successful exploit of this vulnerability may lead to information disclosure. **CVE ID : CVE-2023-25524**		
Vendor: oduyo					
Product: online_collection					
Affected Version(s): * Up to (excluding) 1.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oduyo Online Collection Software allows SQL Injection.This issue affects Online Collection Software: before 1.0.1. **CVE ID : CVE-2023-3716**	N/A	A-ODU-ONLI-210823/1373
Vendor: Omeka					
Product: omeka_s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.0.3					
Unrestricted Upload of File with Dangerous Type	04-Aug-2023	8.8	Unrestricted Upload of File with Dangerous Type in GitHub repository omeka/omeka-s prior to 4.0.3. **CVE ID : CVE-2023-4159**	https://github.com/omeka/omeka-s/commit/2a7fb26452167c8a1d95f207ae5328c6b1b0fcf8, https://huntr.dev/bounties/e2e2365e-6a5f-4ca4-9ef1-297e3ed41f9c	A-OME-OMEK-210823/1374
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository omeka/omeka-s prior to 4.0.3. **CVE ID : CVE-2023-4158**	https://github.com/omeka/omeka-s/commit/2a7fb26452167c8a1d95f207ae5328c6b1b0fcf8, https://huntr.dev/bounties/e0e462ae-d7cb-4a84-b6fe-5f5de20e3d15	A-OME-OMEK-210823/1375
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2023	4.8	Improper Input Validation in GitHub repository omeka/omeka-s prior to 4.0.3. **CVE ID : CVE-2023-4157**	https://github.com/omeka/omeka-s/commit/8b72619d9731b32dd21ab6dcaa01ccc3bbf0db63, https://huntr.dev/bounties/abc3521b-1238-4c4e-97f1-	A-OME-OMEK-210823/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2957db670014	
Vendor: Omron					
Product: cx-programmer					
Affected Version(s): * Up to (including) 9.79					
Use After Free	03-Aug-2023	7.8	Use after free vulnerability exists in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22317 and CVE-2023-22314. **CVE ID : CVE-2023-22277**	N/A	A-OMR-CX-P-210823/1377
Use After Free	03-Aug-2023	7.8	Use after free vulnerability exists in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22277 and CVE-2023-22317. **CVE ID : CVE-2023-22314**	N/A	A-OMR-CX-P-210823/1378
Use After Free	03-Aug-2023	7.8	Use after free vulnerability exists	N/A	A-OMR-CX-P-210823/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22277 and CVE-2023-22314. **CVE ID : CVE-2023-22317**		
Affected Version(s): * Up to (including) 9.80					
Out-of-bounds Read	03-Aug-2023	7.8	Out-of-bounds read vulnerability/issue exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. **CVE ID : CVE-2023-38746**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-005_en.pdf	A-OMR-CX-P-210823/1380
Out-of-bounds Write	03-Aug-2023	7.8	Heap-based buffer overflow vulnerability exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or	https://www.ia.omron.com/product/vulnerability/OMSR-2023-005_en.pdf	A-OMR-CX-P-210823/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution may occur. **CVE ID : CVE-2023-38747**		
Use After Free	03-Aug-2023	7.8	Use after free vulnerability exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. **CVE ID : CVE-2023-38748**	https://www.ia.omron.com/product/vulnerability/OMSR-2023-005_en.pdf	A-OMR-CX-P-210823/1382
Vendor: Oneplus					
Product: store					
Affected Version(s): 3.3.0					
N/A	10-Aug-2023	9.8	A remote code execution vulnerability in the webview component of OnePlus Store app. **CVE ID : CVE-2023-26309**	https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1689464826201645056	A-ONE-STOR-210823/1383
Vendor: online_hospital_management_system_project					
Product: online_hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	10-Aug-2023	9.8	Code-Projects Online Hospital Management System V1.0 is vulnerable to SQL Injection (SQLI) attacks, which allow an attacker to manipulate the SQL	N/A	A-ONL-ONLI-210823/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			queries executed by the application. The application fails to properly validate user-supplied input in the login id and password fields during the login process, enabling an attacker to inject malicious SQL code. **CVE ID : CVE-2023-37069**		
Vendor: online_security_guards_hiring_system_project					
Product: online_security_guards_hiring_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2023	9.8	PHPGurukul Online Security Guards Hiring System v.1.0 is vulnerable to SQL Injection via osghs/admin/search.php. **CVE ID : CVE-2023-39551**	N/A	A-ONL-ONLI-210823/1385
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2023	6.1	PHPGurukul Online Security Guards Hiring System v.1.0 is vulnerable to Cross-Site Scripting (XSS). **CVE ID : CVE-2023-39552**	N/A	A-ONL-ONLI-210823/1386
Vendor: online_shopping_portal_project					
Product: online_shopping_portal					
Affected Version(s): 3.1					
Improper Neutralizat	01-Aug-2023	8.8	Online Shopping Portal Project v3.1	N/A	A-ONL-ONLI-210823/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			was discovered to contain a SQL injection vulnerability via the Email parameter at /shopping/login.php. **CVE ID : CVE-2023-37772**		
Vendor: Open-xchange					
Product: open-xchange_appsuite_backend					
Affected Version(s): * Up to (including) 7.10.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2023	9.8	Full-text autocomplete search allows user-provided SQL syntax to be injected to SQL statements. With existing sanitization in place, this can be abused to trigger benign SQL Exceptions but could potentially be escalated to a malicious SQL injection vulnerability. We now properly encode single quotes for SQL FULLTEXT queries. No publicly available exploits are known. **CVE ID : CVE-2023-26443**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1388
Affected Version(s): * Up to (including) 8.11.0					
Use of Insufficient	02-Aug-2023	7.5	Functions with insufficient randomness were used to generate	https://documentation.open-xchange.com/	A-OPE-OPEN-210823/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			authorization tokens of the integrated oAuth Authorization Service. Authorization codes were predictable for third parties and could be used to intercept and take over the client authorization process. As a result, other users accounts could be compromised. The oAuth Authorization Service is not enabled by default. We have updated the implementation to use sources with sufficient randomness to generate authorization tokens. No publicly available exploits are known. **CVE ID : CVE-2023-26451**	security/advisories/csaf/oxas-adv-2023-0003.json	
Affected Version(s): 7.10.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Aug-2023	4.3	Attackers with access to user accounts can inject arbitrary control characters to SIEVE mail-filter rules. This could be abused to access SIEVE extension that are not allowed by App	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Suite or to inject rules which would break per-user filter processing, requiring manual cleanup of such rules. We have added sanitization to all mail-filter APIs to avoid forwardning control characters to subsystems. No publicly available exploits are known. **CVE ID : CVE-2023-26430**		
Server-Side Request Forgery (SSRF)	02-Aug-2023	3.1	External service lookups for a number of protocols were vulnerable to a time-of-check/time-of-use (TOCTOU) weakness, involving the JDK DNS cache. Attackers that were timing DNS cache expiry correctly were able to inject configuration that would bypass existing network deny-lists. Attackers could exploit this weakness to discover the existence of restricted network infrastructure and service availability. Improvements were made to include deny-lists not only during the check of	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the provided connection data, but also during use. No publicly available exploits are known. **CVE ID : CVE-2023-26438**		
Affected Version(s): 8.10.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Aug-2023	4.3	Attackers with access to user accounts can inject arbitrary control characters to SIEVE mail-filter rules. This could be abused to access SIEVE extension that are not allowed by App Suite or to inject rules which would break per-user filter processing, requiring manual cleanup of such rules. We have added sanitization to all mail-filter APIs to avoid forwardning control characters to subsystems. No publicly available exploits are known. **CVE ID : CVE-2023-26430**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1392
Server-Side Request	02-Aug-2023	3.1	External service lookups for a number of protocols were vulnerable to a	https://documentation.open-xchange.com/	A-OPE-OPEN-210823/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			time-of-check/time-of-use (TOCTOU) weakness, involving the JDK DNS cache. Attackers that were timing DNS cache expiry correctly were able to inject configuration that would bypass existing network deny-lists. Attackers could exploit this weakness to discover the existence of restricted network infrastructure and service availability. Improvements were made to include deny-lists not only during the check of the provided connection data, but also during use. No publicly available exploits are known. **CVE ID : CVE-2023-26438**	security/advisories/csaf/oxas-adv-2023-0003.json	
Affected Version(s): From (including) 8.10.0 Up to (including) 8.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2023	9.8	Full-text autocomplete search allows user-provided SQL syntax to be injected to SQL statements. With existing sanitization in place, this can be abused to trigger benign SQL	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exceptions but could potentially be escalated to a malicious SQL injection vulnerability. We now properly encode single quotes for SQL FULLTEXT queries. No publicly available exploits are known. **CVE ID : CVE-2023-26443**		
Product: open-xchange_appsuite_frontend					
Affected Version(s): * Up to (including) 7.10.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	Frontend themes are defined by user-controllable jslob settings and could point to a malicious resource which gets processed during login. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize the theme	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value and use a default fallback if no theme matches. No publicly available exploits are known. **CVE ID : CVE-2023-26445**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	The users clientID at "application passwords" was not sanitized or escaped before being added to DOM. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize the user-controllable clientID parameter. No publicly available exploits are known. **CVE ID : CVE-2023-26446**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	The "upsell" widget for the portal allows to specify a product description. This description taken from a user-controllable jslob did not get escaped before being added to DOM. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize jslob content. No publicly available exploits are known. **CVE ID : CVE-2023-26447**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1397
Improper Neutralization of Input During Web Page Generation	02-Aug-2023	5.4	Custom log-in and log-out locations are used-defined as jslob but were not checked to contain malicious protocol handlers. Malicious script code can be executed within the	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize jslob content for those locations to avoid redirects to malicious content. No publicly available exploits are known. **CVE ID : CVE-2023-26448**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	The "OX Chat" web service did not specify a media-type when processing responses by external resources. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account or lure a user to a compromised account. We are now defining the accepted media-type to avoid code execution. No publicly available exploits are known. **CVE ID : CVE-2023-26449**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	The "OX Count" web service did not specify a media-type when processing responses by external resources. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We are now defining the accepted media-type to avoid code execution. No publicly available exploits are known.	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26450		
Affected Version(s): From (including) 8.10 Up to (excluding) 8.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	The users clientID at "application passwords" was not sanitized or escaped before being added to DOM. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize the user-controllable clientID parameter. No publicly available exploits are known. **CVE ID : CVE-2023-26446**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1401
Product: open-xchange_appsuite_office					
Affected Version(s): * Up to (excluding) 8.11					
Improper Neutralization of Special	02-Aug-2023	7.8	The cacheservice API could be abused to inject parameters with SQL syntax	https://documentation.open-xchange.com/	A-OPE-OPEN-210823/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			which was insufficiently sanitized before getting executed as SQL statement. Attackers with access to a local or restricted network were able to perform arbitrary SQL queries, discovering other users cached data. We have improved the input check for API calls and filter for potentially malicious content. No publicly available exploits are known. **CVE ID : CVE-2023-26439**	security/advisories/csaf/oxas-adv-2023-0003.json	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2023	7.8	The cacheservice API could be abused to indirectly inject parameters with SQL syntax which was insufficiently sanitized and would later be executed when creating new cache groups. Attackers with access to a local or restricted network could perform arbitrary SQL queries. We have improved the input check for API calls and filter for	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially malicious content. No publicly available exploits are known. **CVE ID : CVE-2023-26440**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2023	5.5	Cacheservice did not correctly check if relative cache object were pointing to the defined absolute location when accessing resources. An attacker with access to the database and a local or restricted network would be able to read arbitrary local file system resources that are accessible by the services system user account. We have improved path validation and make sure that any access is contained to the defined root directory. No publicly available exploits are known. **CVE ID : CVE-2023-26441**	https://documentation.open-xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	A-OPE-OPEN-210823/1404
Server-Side Request	02-Aug-2023	3.2	In case Cacheservice was configured to use a sproxyd object-	https://documentation.open-	A-OPE-OPEN-210823/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			storage backend, it would follow HTTP redirects issued by that backend. An attacker with access to a local or restricted network with the capability to intercept and replay HTTP requests to sproxyd (or who is in control of the sproxyd service) could perform a server-side request-forgery attack and make Cacheservice connect to unexpected resources. We have disabled the ability to follow HTTP redirects when connecting to sproxyd resources. No publicly available exploits are known. **CVE ID : CVE-2023-26442**	xchange.com/security/advisories/csaf/oxas-adv-2023-0003.json	
Vendor: opnsense					
Product: opnsense					
Affected Version(s): * Up to (excluding) 23.7					
Improper Limitation of a Pathname to a Restricted Directory	09-Aug-2023	9.8	A directory traversal vulnerability in the Captive Portal templates of OPNsense before 23.7 allows attackers to execute arbitrary system commands as	https://github.com/opnsense/core/commit/448762d440b51574f1906c0ec2f5ea6dc4f16eb2	A-OPN-OPNS-210823/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			root via a crafted ZIP archive. **CVE ID : CVE-2023-38997**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	9.8	A command injection vulnerability in the component diag_backup.php of OPNsense before 23.7 allows attackers to execute arbitrary commands via a crafted backup configuration file. **CVE ID : CVE-2023-39001**	https://github.com/opnsense/core/commit/e800097d0c287bb665f0751a98a67c75ef7b45e5	A-OPN-OPNS-210823/1407
Incorrect Permission Assignment for Critical Resource	09-Aug-2023	9.8	Insecure permissions in the configuration directory (/conf/) of OPNsense before 23.7 allow attackers to access sensitive information (e.g., hashed root password) which could lead to privilege escalation. **CVE ID : CVE-2023-39004**	N/A	A-OPN-OPNS-210823/1408
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	9.8	A command injection vulnerability in the component /api/cron/settings/setJob/ of OPNsense before 23.7 allows attackers to execute arbitrary system commands. **CVE ID : CVE-2023-39008**	https://github.com/opnsense/core/commit/e800097d0c287bb665f0751a98a67c75ef7b45e5	A-OPN-OPNS-210823/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2023	9.6	/ui/cron/item/open in the Cron component of OPNsense before 23.7 allows XSS. **CVE ID : CVE-2023-39007**	https://github.com/opnsense/core/commit/5edff49db1cd8b5078611e2f542d91c02af2b25c	A-OPN-OPNS-210823/1410
Incorrect Permission Assignment for Critical Resource	09-Aug-2023	7.5	OPNsense before 23.7 was discovered to contain insecure permissions in the directory /tmp. **CVE ID : CVE-2023-39003**	N/A	A-OPN-OPNS-210823/1411
Incorrect Permission Assignment for Critical Resource	09-Aug-2023	7.5	Insecure permissions exist for configd.socket in OPNsense before 23.7. **CVE ID : CVE-2023-39005**	https://github.com/opnsense/core/issues/6647	A-OPN-OPNS-210823/1412
Cross-Site Request Forgery (CSRF)	09-Aug-2023	6.5	A Cross-Site Request Forgery (CSRF) in the System Halt API (/system/halt) of OPNsense before 23.7 allows attackers to cause a Denial of Service (DoS) via a crafted GET request. **CVE ID : CVE-2023-38999**	https://github.com/opnsense/core/commit/5d68f43d1f254144831881fc87d885eed120cf3c	A-OPN-OPNS-210823/1413
URL Redirection to Untrusted Site ('Open Redirect')	09-Aug-2023	6.1	An open redirect in the Login page of OPNsense before 23.7 allows attackers to redirect a victim user to an arbitrary	https://github.com/opnsense/core/commit/6bc025af1705dcdd8ef22ff5d4fcb986fa4e45f8	A-OPN-OPNS-210823/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web site via a crafted URL. **CVE ID : CVE-2023-38998**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in the component /ui/diagnostics/log/core/ of OPNsense before 23.7 allows attackers to inject arbitrary JavaScript via the URL path. **CVE ID : CVE-2023-39000**	https://github.com/opnsense/core/commit/d1f350ce70e477adc86d445f5cda9b24f9ff0168	A-OPN-OPNS-210823/1415
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2023	6.1	A cross-site scripting (XSS) vulnerability in the act parameter of system_certmanager.php in OPNsense before 23.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-39002**	https://github.com/opnsense/core/commit/a4f6a8f8d604271f81984cfcbba0471af58e34dc	A-OPN-OPNS-210823/1416
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2023	5.4	The Crash Reporter (crash_reporter.php) component of OPNsense before 23.7 mishandles input sanitization. **CVE ID : CVE-2023-39006**	https://github.com/opnsense/core/commit/1c05a19d9d52c7bfa4ac52114935d9fe76d5d181	A-OPN-OPNS-210823/1417
Vendor: oppo					
Product: oppo_store					
Affected Version(s): 1.5.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Aug-2023	9.8	A remote code execution vulnerability in the webview component of OPPO Store app. **CVE ID : CVE-2023-26311**	https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1689584995217448960	A-OPP-OPPO-210823/1418
Vendor: Oxid-esales					
Product: eshop					
Affected Version(s): From (including) 6.5.0 Up to (excluding) 6.5.3					
Unrestricted Upload of File with Dangerous Type	02-Aug-2023	5.3	OXID eShop Enterprise Edition 6.5.0 – 6.5.2 before 6.5.3 allows uploading files with modified headers in the administration area. An attacker can upload a file with a modified header to create a HTTP Response Splitting attack. **CVE ID : CVE-2023-38330**	https://docs.oxid-esales.com/de/security/security-bulletins.html#security-bulletin-2023-002, https://bugs.oxid-esales.com/view.php?id=7479	A-OXI-ESHO-210823/1419
Vendor: Paessler					
Product: prtg_network_monitor					
Affected Version(s): * Up to (excluding) 23.3.86.1520					
Cross-Site Request Forgery (CSRF)	09-Aug-2023	8.8	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760 x64. The NetApp Volume Sensor transmits cleartext credentials over the network when the HTTP protocol is selected.	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-monitor-23-3-86-1520	A-PAE-PRTG-210823/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This can be triggered remotely via a CSRF by simply sending a controls/addsensor3.htm link to a logged-in victim. **CVE ID : CVE-2023-31452**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	7.2	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760. Due to command-line parameter injection and an undocumented debug feature flag, an attacker can utilize the HL7 sensor to write arbitrary data to the disk. This can be utilized to write a custom EXE(.bat) sensor, that will then run. This primitive gives remote code execution. **CVE ID : CVE-2023-32781**	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-monitor-23-3-86-1520	A-PAE-PRTG-210823/1421
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	7.2	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760. Due to command-line parameter injection and an undocumented debug feature flag, an attacker can utilize the DICOM	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-monitor-23-3-86-1520	A-PAE-PRTG-210823/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensor to write arbitrary data to the disk. This can be utilized to write a custom EXE(.bat) sensor, that will then run. This primitive gives remote code execution. **CVE ID : CVE-2023-32782**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Aug-2023	4.7	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760 x64. To exploit the vulnerability, a authenticated user can create a HL7 Sensor. When creating this sensor, the user can set the HL7 message that should be sent from the PRTG device. This input parameter contains a path traversal vulnerability that allows an attacker to choose arbitrary files from the system. **CVE ID : CVE-2023-31448**	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-monitor-23-3-86-1520	A-PAE-PRTG-210823/1423
Improper Limitation of a Pathname to a Restricted Directory	09-Aug-2023	4.7	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760 x64. To exploit the vulnerability, a authenticated user	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-	A-PAE-PRTG-210823/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			can create a WMI Custom Sensor. When creating this sensor, the user can set the WQL message that should be sent from the PRTG device. This input parameter contains a path traversal vulnerability that allows an attacker to choose arbitrary files from the system. **CVE ID : CVE-2023-31449**	monitor-23-3-86-1520	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Aug-2023	4.7	An issue was discovered in Paessler PRTG Network Monitor 23.2.83.1760 x64. To exploit the vulnerability, a authenticated user can create a SQL Sensor. When creating this sensor, the user can set the SQL message that should be sent from the PRTG device. This input parameter contains a path traversal vulnerability that allows an attacker to choose arbitrary files from the system. They will be transmitted over the internet to the attacker's machine.	https://kb.paessler.com/en/topic/91845-multiple-vulnerabilites-fixed-in-paessler-prtg-network-monitor-23-3-86-1520	A-PAE-PRTG-210823/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31450		
Vendor: palantir					
Product: foundry					
Affected Version(s): * Up to (excluding) 6.228.0					
N/A	03-Aug-2023	4.3	A security defect was discovered in Foundry Issues that enabled users to create convincing phishing links by editing the request sent when creating an Issue. This defect was resolved in Frontend release 6.228.0 . **CVE ID : CVE-2023-30952**	https://palantir.safebase.us/?tcuUid=42bdb7fa-9a6d-4462-b89d-cabc62f281f4	A-PAL-FOUN-210823/1426
Product: foundry_campaigns					
Affected Version(s): * Up to (excluding) 0.623.0					
Missing Authorization	03-Aug-2023	5.9	The foundry campaigns service was found to be vulnerable to an unauthenticated information disclosure in a rest endpoint **CVE ID : CVE-2023-30950**	https://palantir.safebase.us/?tcuUid=d839709d-c50f-4a37-8faa-b0c35054418a	A-PAL-FOUN-210823/1427
Product: magritte-rest-source-bundle					
Affected Version(s): * Up to (excluding) 7.210.0					
Improper Restriction of XML External Entity Reference	03-Aug-2023	6.5	The Foundry Magritte plugin rest-source was found to be vulnerable to an an XML external Entity attack (XXE).	https://palantir.safebase.us/?tcuUid=fe021f28-9e25-42c4-acd8-	A-PAL-MAGR-210823/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30951	772cd8006ced	
Vendor: Papercut					
Product: papercut_mf					
Affected Version(s): * Up to (excluding) 22.1.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2023	9.8	PaperCut NG and PaperCut MF before 22.1.3 on Windows allow path traversal, enabling attackers to upload, read, or delete arbitrary files. This leads to remote code execution when external device integration is enabled (a very common configuration). **CVE ID : CVE-2023-39143**	https://www.papercut.com/kb/Main/securitybulletinjuly2023/	A-PAP-PAPE-210823/1429
Product: papercut_ng					
Affected Version(s): * Up to (excluding) 22.1.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2023	9.8	PaperCut NG and PaperCut MF before 22.1.3 on Windows allow path traversal, enabling attackers to upload, read, or delete arbitrary files. This leads to remote code execution when external device integration is enabled (a very common configuration). **CVE ID : CVE-2023-39143**	https://www.papercut.com/kb/Main/securitybulletinjuly2023/	A-PAP-PAPE-210823/1430
Vendor: paymentsplugin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_full_stripe_free					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology WP Full Stripe Free plugin <= 1.6.1 versions. **CVE ID : CVE-2023-28934**	N/A	A-PAY-WP_F-210823/1431
Vendor: pega					
Product: pega_platform					
Affected Version(s): From (including) 6.1 Up to (including) 7.3.1					
Improper Authentication	07-Aug-2023	9.8	Pega platform clients who are using versions 6.1 through 7.3.1 may be utilizing default credentials **CVE ID : CVE-2023-32090**	https://support.pega.com/support-doc/pega-security-advisory-%E2%80%93-c23-vulnerability-default-operators	A-PEG-PEGA-210823/1432
Vendor: pharmacy_management_system_project					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	06-Aug-2023	9.8	A vulnerability was found in SourceCodester Pharmacy Management System 1.0. It has been declared as critical. Affected by this	N/A	A-PHA-PHAR-210823/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is an unknown functionality of the file manage_website.php. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236221 was assigned to this vulnerability. **CVE ID : CVE-2023-4186**		
Vendor: Phpjabbers					
Product: availability_booking_calendar					
Affected Version(s): 5.0					
N/A	04-Aug-2023	9.8	PHPJabbers Availability Booking Calendar 5.0 is vulnerable to Incorrect Access Control due to improper input validation of password parameter. **CVE ID : CVE-2023-36131**	N/A	A-PHP-AVAI-210823/1434
N/A	04-Aug-2023	9.8	PHP Jabbers Availability Booking Calendar 5.0 is vulnerable to Incorrect Access Control. **CVE ID : CVE-2023-36132**	N/A	A-PHP-AVAI-210823/1435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Aug-2023	9.8	PHPJabbers Availability Booking Calendar 5.0 is vulnerable to User Account Takeover through username/password change. **CVE ID : CVE-2023-36133**	N/A	A-PHP-AVAI-210823/1436
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability has been found in PHP Jabbers Availability Booking Calendar 5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument session_id leads to cross site scripting. The attack can be launched remotely. The identifier VDB-235957 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4110**	N/A	A-PHP-AVAI-210823/1437
Product: bus_reservation_system					
Affected Version(s): 1.1					
Improper Neutralizat	03-Aug-2023	6.1	A vulnerability was found in PHP Jabbers	N/A	A-PHP-BUS_-210823/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Bus Reservation System 1.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index/pickup_id leads to cross site scripting. The attack may be launched remotely. VDB-235958 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4111**		
Product: callback_widget					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the value-text-o_sms_email_request_message parameters of index.php in PHPJabbers Callback Widget v1.0. **CVE ID : CVE-2023-36314**	N/A	A-PHP-CALL-210823/1439
Improper Neutralization of	10-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the	N/A	A-PHP-CALL-210823/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			"action" parameter of index.php in PHPJabbers Callback Widget v1.0. **CVE ID : CVE-2023-36315**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	5.4	There is a Cross Site Scripting (XSS) vulnerability in the value-enum-o_bf_include_timezone parameter of index.php in PHPJabbers Callback Widget v1.0. **CVE ID : CVE-2023-36312**	N/A	A-PHP-CALL-210823/1441
Product: catering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	PHPJabbers Catering System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /index.php?controller=pjAdmin&action=pjActionForgot. **CVE ID : CVE-2023-34869**	N/A	A-PHP-CATE-210823/1442
Product: class_scheduling_system					
Affected Version(s): 1.0					
Insufficient Verification of Data Authenticity	04-Aug-2023	9.8	In PHP Jabbers Class Scheduling System 1.0, lack of verification when changing an email address and/or password (on the Profile Page) allows	N/A	A-PHP-CLAS-210823/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to take over accounts. **CVE ID : CVE-2023-36134**		
N/A	04-Aug-2023	7.5	User enumeration is found in in PHPJabbers Class Scheduling System v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users. **CVE ID : CVE-2023-36135**	N/A	A-PHP-CLAS-210823/1444
Cleartext Storage of Sensitive Informatio n	08-Aug-2023	6.5	PHPJabbers Class Scheduling System 1.0 lacks encryption on the password when editing a user account (update user page) allowing an attacker to capture all user names and passwords in clear text. **CVE ID : CVE-2023-36136**	N/A	A-PHP-CLAS-210823/1445
Improper Neutralizat ion of Input During Web Page Generation	04-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Class Scheduling System 1.0.	N/A	A-PHP-CLAS-210823/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-36137**		
Product: cleaning_business_software					
Affected Version(s): 1.0					
Insufficient Verification of Data Authenticity	04-Aug-2023	9.8	In PHPJabbers Cleaning Business Software 1.0, lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts. **CVE ID : CVE-2023-36139**	N/A	A-PHP-CLEA-210823/1447
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2023	6.1	PHPJabbers Cleaning Business Software 1.0 is vulnerable to Cross Site Scripting (XSS) via the theme parameter of preview.php. **CVE ID : CVE-2023-36138**	N/A	A-PHP-CLEA-210823/1448
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability classified as problematic has been found in PHP Jabbers Cleaning Business 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument index leads to cross site scripting. It is possible to launch the attack remotely. VDB-235962 is the identifier assigned to	N/A	A-PHP-CLEA-210823/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4115**		
N/A	04-Aug-2023	5.3	User enumeration is found in in PHPJabbers Cleaning Business Software 1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users. **CVE ID : CVE-2023-36141**	N/A	A-PHP-CLEA-210823/1450
Product: document_creator					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-2023	9.8	There is a SQL injection (SQLi) vulnerability in the "column" parameter of index.php in PHPJabbers Document Creator v1.0. **CVE ID : CVE-2023-36311**	N/A	A-PHP-DOCU-210823/1451
Improper Neutralization of Input	10-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the "action" parameter	N/A	A-PHP-DOCU-210823/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			of index.php in PHPJabbers Document Creator v1.0. **CVE ID : CVE-2023-36309**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the "column" parameter of index.php in PHPJabbers Document Creator v1.0. **CVE ID : CVE-2023-36310**	N/A	A-PHP-DOCU-210823/1453
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	PHPJabbers Document Creator v1.0 is vulnerable to Cross Site Scripting (XSS) via all post parameters of "Export Requests" aside from "request_feed". **CVE ID : CVE-2023-36313**	N/A	A-PHP-DOCU-210823/1454
Product: night_club_booking_software					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability was found in PHP Jabbers Night Club Booking Software 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /index.php. The manipulation of the argument index leads to cross site	N/A	A-PHP-NIGH-210823/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack may be initiated remotely. The identifier VDB-235961 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4114**		
Product: rental_property_booking_calendar					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability, which was classified as problematic, has been found in PHP Jabbers Rental Property Booking 2.0. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235964. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-PHP-RENT-210823/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4117		
Product: service_booking_script					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability was found in PHP Jabbers Service Booking Script 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-235960. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4113**	N/A	A-PHP-SERV-210823/1457
Product: shuttle_booking_software					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability was found in PHP Jabbers Shuttle Booking Software 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php. The manipulation leads to cross site	N/A	A-PHP-SHUT-210823/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-235959. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4112**		
Product: taxi_booking_script					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability classified as problematic was found in PHP Jabbers Taxi Booking 2.0. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235963. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4116**	N/A	A-PHP-TAXI-210823/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ticket_support_script					
Affected Version(s): 3.2					
Unrestricted Upload of File with Dangerous Type	10-Aug-2023	9.8	A File Upload vulnerability in PHPJabbers Ticket Support Script v3.2 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID : CVE-2023-39776**	N/A	A-PHP-TICK-210823/1460
Product: time_slots_booking_calendar					
Affected Version(s): 3.3					
N/A	01-Aug-2023	9.8	Improper input validation of password parameter in PHP Jabbers Time Slots Booking Calendar v 3.3 results in insecure passwords. **CVE ID : CVE-2023-33561**	N/A	A-PHP-TIME-210823/1461
N/A	01-Aug-2023	9.8	User enumeration is found in in PHP Jabbers Time Slots Booking Calendar v3.3. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users. **CVE ID : CVE-2023-33562**	N/A	A-PHP-TIME-210823/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	01-Aug-2023	8.8	In PHP Jabbers Time Slots Booking Calendar 3.3 , lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts. **CVE ID : CVE-2023-33563**	N/A	A-PHP-TIME-210823/1463
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in "cid" parameter of preview.php in PHPJabbers Time Slots Booking Calendar v3.3. **CVE ID : CVE-2023-33560**	N/A	A-PHP-TIME-210823/1464
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Time Slots Booking Calendar v3.3. **CVE ID : CVE-2023-33564**	N/A	A-PHP-TIME-210823/1465
Product: yacht_listing_script					
Affected Version(s): 1.0					
Exposure of Resource to Wrong Sphere	10-Aug-2023	7.5	An information leak in PHPJabbers Yacht Listing Script v1.0 allows attackers to export clients' credit card numbers from	N/A	A-PHP-YACH-210823/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Reservations module. **CVE ID : CVE-2023-38830**		
Vendor: pierre-jehan					
Product: owl_carousel					
Affected Version(s): * Up to (including) 0.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pierre JEHAN Owl Carousel plugin <= 0.5.3 versions. **CVE ID : CVE-2023-23829**	N/A	A-PIE-OWL_-210823/1467
Vendor: Pimcore					
Product: customer_data_framework					
Affected Version(s): * Up to (excluding) 3.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/customer-data-framework prior to 3.4.2. **CVE ID : CVE-2023-4145**	https://github.com/pimcore/customer-data-framework/commit/72f45dd537a706954e7a71c99fbe318640e846a2, https://huntr.dev/bounties/ce852777-2994-40b4-bb4e-c4d10023eeb0	A-PIM-CUST-210823/1468
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.6.7					
Improper Limitation	04-Aug-2023	8.8	Pimcore is an Open Source Data &	https://github.com/pimcore	A-PIM-PIMC-210823/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Experience Management Platform: PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce. A path traversal vulnerability exists in the `AssetController::importServerFilesAction`, which allows an attacker to overwrite or modify sensitive files by manipulating the pimcore_log parameter.This can lead to potential denial of service---key file overwrite. The impact of this vulnerability allows attackers to: overwrite or modify sensitive files, potentially leading to unauthorized access, privilege escalation, or disclosure of confidential information. This could also cause a denial of service (DoS) if critical system files are overwritten or deleted. **CVE ID : CVE-2023-38708**	/pimcore/security/advisories/GHSA-34hj-v8fm-x887, https://github.com/pimcore/pimcore/commit/58012d0e3b8b926fb54eccbd64ec5c993b30c22c	
Vendor: pnpm					
Product: pnpm					
Affected Version(s): * Up to (excluding) 7.33.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Aug-2023	9.8	pnpm is a package manager. It is possible to construct a tarball that, when installed via npm or parsed by the registry is safe, but when installed via pnpm is malicious, due to how pnpm parses tar archives. This can result in a package that appears safe on the npm registry or when installed via npm being replaced with a compromised or malicious version when installed via pnpm. This issue has been patched in version(s) 7.33.4 and 8.6.8. **CVE ID : CVE-2023-37478**	https://github.com/pnpm/pnpm/security/advisories/GHSA-5r98-f33j-g8h7	A-PNP-PNPM-210823/1470
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.6.8					
N/A	01-Aug-2023	9.8	pnpm is a package manager. It is possible to construct a tarball that, when installed via npm or parsed by the registry is safe, but when installed via pnpm is malicious, due to how pnpm parses tar archives. This can result in a package that appears safe on the npm registry or when installed via npm	https://github.com/pnpm/pnpm/security/advisories/GHSA-5r98-f33j-g8h7	A-PNP-PNPM-210823/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being replaced with a compromised or malicious version when installed via pnpm. This issue has been patched in version(s) 7.33.4 and 8.6.8. **CVE ID : CVE-2023-37478**		
Vendor: postsnippets					
Product: post_snippets					
Affected Version(s): * Up to (excluding) 4.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Postsnippets Post Snippets plugin <= 4.0.2 versions. **CVE ID : CVE-2023-25459**	N/A	A-POS-POST-210823/1472
Vendor: pragmaticmates					
Product: realia					
Affected Version(s): * Up to (including) 1.4.0					
Cross-Site Request Forgery (CSRF)	10-Aug-2023	6.5	The Realia plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.4.0. This is due to missing nonce validation on the 'process_change_profile_form' function. This makes it possible for unauthenticated attackers to change user email via a	https://plugins.trac.wordpress.org/browser/realia/tags/1.4.0/includes/post-types/class-realia-post-type-user.php#L112	A-PRA-REAL-210823/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4277**		
Vendor: Prestashop					
Product: prestashop					
Affected Version(s): * Up to (excluding) 1.7.8.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to remote code execution through SQL injection and arbitrary file write in the back office. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds. **CVE ID : CVE-2023-39526**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-gf46-prm4-56pc, https://github.com/PrestaShop/PrestaShop/commit/817847e2347844a9b6add017581f1932bcd28c09	A-PRE-PRES-210823/1474
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	6.1	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to cross-site scripting through the `isCleanHTML` method. Versions	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-xw2r-f8xv-c8xp, https://github.com/PrestaShop/PrestaShop/commit/af	A-PRE-PRES-210823/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds. **CVE ID : CVE-2023-39527**	c14f8eaa058b3e6a20ac43e033ee2656fb88b4	
Affected Version(s): * Up to (excluding) 8.1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, SQL injection possible in the product search field, in BO's product page. Version 8.1.1 contains a patch for this issue. There are no known workarounds. **CVE ID : CVE-2023-39524**	https://github.com/PrestaShop/PrestaShop/commit/2047d4c053043102bc46a37d383b392704bf14d7, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-75p5-jwx4-qw9h	A-PRE-PRES-210823/1476
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Aug-2023	9.1	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, in the back office, files can be compromised using path traversal by replaying the import file deletion query with a specified file path that uses the traversal path. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-m9r4-3fg7-pqm2, https://github.com/PrestaShop/PrestaShop/commit/c7c9a5110421bb2856f4d312ecce192d079b5ec7	A-PRE-PRES-210823/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39525		
N/A	07-Aug-2023	9.1	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, it is possible to delete a file from the server by using the Attachments controller and the Attachments API. Version 8.1.1 contains a patch for this issue. There are no known workarounds. **CVE ID : CVE-2023-39529**	https://github.com/PrestaShop/PrestaShop/commit/b08c647305dc1e9e6a2445b724d13a9733b6ed82, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-2rf5-3fw8-qm47	A-PRE-PRES-210823/1478
Improper Input Validation	07-Aug-2023	9.1	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, it is possible to delete files from the server via the CustomerMessage API. Version 8.1.1 contains a patch for this issue. There are no known workarounds. **CVE ID : CVE-2023-39530**	https://github.com/PrestaShop/PrestaShop/commit/6ce750b2367a7309b6bf50166f1873cb86ad57e9, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-v4gr-v679-42p7	A-PRE-PRES-210823/1479
Improper Limitation of a Pathname to a Restricted	07-Aug-2023	8.6	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, the `displayAjaxEmailHT	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-hpf4-v7v2-	A-PRE-PRES-210823/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			ML` method can be used to read any file on the server, potentially even outside of the project if the server is not correctly configured. Version 8.1.1 contains a patch for this issue. There are no known workarounds. **CVE ID : CVE-2023-39528**	95p2, https://github.com/PrestaShop/PrestaShop/commit/11de3a84322fa4ecd0995ac40d575db61804724c	
Affected Version(s): 8.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to remote code execution through SQL injection and arbitrary file write in the back office. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds. **CVE ID : CVE-2023-39526**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-gf46-prm4-56pc, https://github.com/PrestaShop/PrestaShop/commit/817847e2347844a9b6add017581f1932bcd28c09	A-PRE-PRES-210823/1481
Improper Neutralization of Input During Web Page Generation	07-Aug-2023	6.1	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to cross-site scripting	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-xw2r-f8xv-c8xp, https://github	A-PRE-PRES-210823/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			through the `isCleanHTML` method. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds. **CVE ID : CVE-2023-39527**	.com/PrestaShop/PrestaShop/commit/afc14f8eaa058b3e6a20ac43e033ee2656fb88b4	
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to remote code execution through SQL injection and arbitrary file write in the back office. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds. **CVE ID : CVE-2023-39526**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-gf46-prm4-56pc, https://github.com/PrestaShop/PrestaShop/commit/817847e2347844a9b6add017581f1932bcd28c09	A-PRE-PRES-210823/1483
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	6.1	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to cross-site scripting through the `isCleanHTML` method. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch.	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-xw2r-f8xv-c8xp, https://github.com/PrestaShop/PrestaShop/commit/afc14f8eaa058b3e6a20ac43e	A-PRE-PRES-210823/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds. **CVE ID : CVE-2023-39527**	033ee2656fb88b4	
Vendor: procps_project					
Product: procps					
Affected Version(s): From (including) 3.3.0 Up to (including) 4.0.3					
Out-of-bounds Write	02-Aug-2023	5.5	Under some circumstances, this weakness allows a user who has access to run the “ps” utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap. **CVE ID : CVE-2023-4016**	N/A	A-PRO-PROC-210823/1485
Vendor: profosbox					
Product: agp_font_awesome_collection					
Affected Version(s): * Up to (including) 3.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alexey Golubnichenko AGP Font Awesome Collection plugin <= 3.2.4 versions. **CVE ID : CVE-2023-30481**	N/A	A-PRO-AGP_-210823/1486
Vendor: projectdiscovery					
Product: nuclei					
Affected Version(s): * Up to (excluding) 2.9.9					
Improper Limitation of a	04-Aug-2023	7.5	Nuclei is a vulnerability scanner. Prior to	https://github.com/projectdiscovery/nucl	A-PRO-NUCL-210823/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			version 2.9.9, a security issue in the Nuclei project affected users utilizing Nuclei as Go code (SDK) running custom templates. This issue did not affect CLI users. The problem was related to sanitization issues with payload loading in sandbox mode. There was a potential risk with payloads loading in sandbox mode. The issue occurred due to relative paths not being converted to absolute paths before doing the check for `sandbox` flag allowing arbitrary files to be read on the filesystem in certain cases when using Nuclei from `Go` SDK implementation. This issue has been fixed in version 2.9.9. The maintainers have also enabled sandbox by default for filesystem loading. This can be optionally disabled if required. The `-sandbox` option has been deprecated and is now divided into	ei/security/advisories/GHSA-2xx4-jj5v-6mff	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			two new options: `-lfa` (allow local file access) which is enabled by default and `-lna` (restrict local network access) which can be enabled by users optionally. The `-lfa` allows file (payload) access anywhere on the system (disabling sandbox effectively), and `-lna` blocks connections to the local/private network. **CVE ID : CVE-2023-37896**		
Vendor: pyrocms					
Product: pyrocms					
Affected Version(s): 3.9					
N/A	04-Aug-2023	9.8	PyroCMS 3.9 contains a remote code execution (RCE) vulnerability that can be exploited through a server-side template injection (SSTI) flaw. This vulnerability allows a malicious attacker to send customized commands to the server and execute arbitrary code on the affected system. **CVE ID : CVE-2023-29689**	N/A	A-PYR-PYRO-210823/1488
Vendor: Qemu					
Product: qemu					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	03-Aug-2023	6.5	A flaw was found in the QEMU virtual crypto device while handling data encryption/decryption requests in virtio_crypto_handle_sym_req. There is no check for the value of `src_len` and `dst_len` in virtio_crypto_sym_op_helper, potentially leading to a heap buffer overflow when the two values differ. **CVE ID : CVE-2023-3180**	https://bugzilla.redhat.com/show_bug.cgi?id=2222424	A-QEM-QEMU-210823/1489
Affected Version(s): * Up to (excluding) 2023-08-03					
Out-of-bounds Read	04-Aug-2023	6.5	A heap out-of-bounds memory read flaw was found in the virtual nvme device in QEMU. The QEMU process does not validate an offset provided by the guest before computing a host heap pointer, which is used for copying data back to the guest. Arbitrary heap memory relative to an allocated buffer can be disclosed. **CVE ID : CVE-2023-4135**	https://bugzilla.redhat.com/show_bug.cgi?id=2229101	A-QEM-QEMU-210823/1490
Vendor: quic_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: quic					
Affected Version(s): * Up to (excluding) 0.37.2					
Allocation of Resources Without Limits or Throttling	08-Aug-2023	7.5	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no known workarounds for this issue. **CVE ID : CVE-2023-39533**	https://github.com/libp2p/go-libp2p/commit/e30fcf7dfd4715ed89a5e68d7a4f774d3b9aa92d, https://github.com/libp2p/go-libp2p/pull/2454, https://github.com/quic-go/quic-go/pull/4012, https://github.com/libp2p/go-libp2p/security/advisories/GHSA-876p-8259-xjgg	A-QUI-QUIC-210823/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: rankmath					
Product: seo					
Affected Version(s): * Up to (excluding) 1.0.119.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Rank Math SEO plugin <= 1.0.119 versions. **CVE ID : CVE-2023-32600**	N/A	A-RAN-SEO-210823/1492
Vendor: ransomchristofferson					
Product: pdq_csv					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ransom Christofferson PDQ CSV plugin <= 1.0.0 versions. **CVE ID : CVE-2023-31221**	N/A	A-RAN-PDQ_-210823/1493
Vendor: rconfig					
Product: rconfig					
Affected Version(s): 3.9.4					
Server-Side Request Forgery (SSRF)	01-Aug-2023	8.8	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path_b parameter in the doDiff Function of /classes/compareClass.php. This vulnerability allows authenticated attackers to make	N/A	A-RCO-RCON-210823/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary requests via injection of crafted URLs. **CVE ID : CVE-2023-39108**		
Server-Side Request Forgery (SSRF)	01-Aug-2023	8.8	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path_a parameter in the doDiff Function of /classes/compareClass.php. This vulnerability allows authenticated attackers to make arbitrary requests via injection of crafted URLs. **CVE ID : CVE-2023-39109**	N/A	A-RCO-RCON-210823/1495
Server-Side Request Forgery (SSRF)	01-Aug-2023	8.8	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path parameter at /ajaxGetFileByPath.php. This vulnerability allows authenticated attackers to make arbitrary requests via injection of crafted URLs. **CVE ID : CVE-2023-39110**	N/A	A-RCO-RCON-210823/1496
Vendor: rdkcentral					
Product: rdk-b					
Affected Version(s): 2022q3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-RDK-RDK--210823/1497
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	A-RDK-RDK--210823/1498
Vendor: Redhat					
Product: keycloak					
Affected Version(s): * Up to (excluding) 18.0.6					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication,	https://access.redhat.com/security/cve/C	A-RED-KEYC-210823/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	VE-2023-0264	
Product: openshift_container_platform					
Affected Version(s): 4.10					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality,	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability. **CVE ID : CVE-2023-0264**		
Affected Version(s): 4.9					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1501
Product: openshift_container_platform_for_ibm_linuxone					
Affected Version(s): 4.10					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**		
Affected Version(s): 4.9					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1503
Product: openshift_container_platform_ibm_z_systems					
Affected Version(s): 4.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1504
Affected Version(s): 4.9					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-OPEN-210823/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**		
Product: single_sign-on					
Affected Version(s): -					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-SING-210823/1506
Affected Version(s): * Up to (excluding) 7.6.2					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated	https://access.redhat.com/security/cve/CVE-2023-0264	A-RED-SING-210823/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**		
Vendor: renjikai					
Product: linuxasmcallgraph					
Affected Version(s): * Up to (excluding) 2022-02-08					
Unrestricted Upload of File with Dangerous Type	04-Aug-2023	9.8	LinuxASMCallGraph is software for drawing the call graph of the programming code. Linux ASMCallGraph before commit 20dba06bd1a3cf260612d4f21547c25002121cd5 allows attackers to cause a remote code execution on the server side via uploading a crafted ZIP file due to incorrect filtering rules of uploaded file. The problem has been patched in commit 20dba06bd1a3cf260612d4f21547c25002	https://github.com/bjrjk/LinuxASMCallGraph/security/advisories/GHSA-63c3-r9qm-c2wx, https://github.com/bjrjk/LinuxASMCallGraph/commit/20dba06bd1a3cf260612d4f21547c25002121cd5	A-REN-LINU-210823/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			121cd5. There are no known workarounds. **CVE ID : CVE-2023-39346**		
Vendor: resort_reservation_system_project					
Product: resort_reservation_system					
Affected Version(s): 1.0					
External Control of File Name or Path	06-Aug-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Resort Reservation System 1.0. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-236234 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-4191**	N/A	A-RES-RESO-210823/1509
Improper Neutralization of Special Elements used in an SQL Command	07-Aug-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Resort Reservation System 1.0. This affects an unknown part of the file manage_user.php. The manipulation of	N/A	A-RES-RESO-210823/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			the argument id 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-236235. **CVE ID : CVE-2023-4192**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-2023	9.8	A vulnerability has been found in SourceCodester Resort Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_fee.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. The identifier of this vulnerability is VDB-236236. **CVE ID : CVE-2023-4193**	N/A	A-RES-RESO-210823/1511
Vendor: rigorous-digital					
Product: dovetail					
Affected Version(s): * Up to (including) 1.2.13					
Improper Neutralization of	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-RIG-DOVE-210823/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Rigorous & Factory Pattern Dovetail plugin <= 1.2.13 versions. **CVE ID : CVE-2023-25984**		
Vendor: riverside					
Product: http_headers					
Affected Version(s): * Up to (including) 1.18.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Dimitar Ivanov HTTP Headers plugin <= 1.18.11 versions. **CVE ID : CVE-2023-37874**	N/A	A-RIV-HTTP-210823/1513
Vendor: rs485					
Product: logisticspipes					
Affected Version(s): From (including) 0.7.0.91 Up to (excluding) 0.10.0.71					
Deserialization of Untrusted Data	04-Aug-2023	9.8	Logistics Pipes is a modification (a.k.a. mod) for the computer game Minecraft Java Edition. The mod used Java's `ObjectInputStream#readObject` on untrusted data coming from clients or servers over the network resulting in possible remote code execution when sending specifically crafted network packets after connecting. The	https://github.com/RS485/LogisticsPipes/commit/39a90b8f2d1a2bcc512ec68c3e139f1dac07aa56, https://github.com/RS485/LogisticsPipes/security/advisories/GHSA-mcp7-xf3v-25x3	A-RS4-LOGI-210823/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected versions were released between 2013 and 2016 and the issue (back then unknown) was fixed in 2016 by a refactoring of the network IO code. The issue is present in all Logistics Pipes versions ranged from 0.7.0.91 prior to 0.10.0.71, which were downloaded from different platforms summing up to multi-million downloads. For Minecraft version 1.7.10 the issue was fixed in build 0.10.0.71. Everybody on Minecraft 1.7.10 should check their version number of Logistics Pipes in their modlist and update, if the version number is smaller than 0.10.0.71. Any newer supported Minecraft version (like 1.12.2) never had a Logistics Pipes version with vulnerable code. The best available workaround for vulnerable versions is to play in singleplayer only or update to newer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Minecraft versions and modpacks. **CVE ID : CVE-2023-38689**		
Vendor: rust-lang					
Product: cargo					
Affected Version(s): * Up to (excluding) 0.72.2					
Insecure Preserved Inherited Permissions	04-Aug-2023	7.3	Cargo downloads the Rust project's dependencies and compiles the project. Cargo prior to version 0.72.2, bundled with Rust prior to version 1.71.1, did not respect the umask when extracting crate archives on UNIX-like systems. If the user downloaded a crate containing files writeable by any local user, another local user could exploit this to change the source code compiled and executed by the current user. To prevent existing cached extractions from being exploitable, the Cargo binary version 0.72.2 included in Rust 1.71.1 or later will purge caches generated by older Cargo versions automatically. As a workaround,	https://github.com/rust-lang/cargo/pull/12443, https://github.com/rust-lang/cargo/commit/d78bbf4bde3c6b95caca7512f537c6f9721426ff, https://github.com/rust-lang/cargo/security/advisories/GHSA-j3xp-wfr4-hx87	A-RUS-CARG-210823/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configure one's system to prevent other local users from accessing the Cargo directory, usually located in `~/.cargo`. **CVE ID : CVE-2023-38497**		
Vendor: RWS					
Product: worldserver					
Affected Version(s): * Up to (excluding) 11.8.0					
Insufficient Entropy	01-Aug-2023	5.3	Session tokens in RWS WorldServer 11.7.3 and earlier have a low entropy and can be enumerated, leading to unauthorized access to user sessions. **CVE ID : CVE-2023-38357**	N/A	A-RWS-WORL-210823/1516
Vendor: Samsung					
Product: galaxy_store					
Affected Version(s): * Up to (excluding) 4.5.56.6					
Incorrect Authorization	10-Aug-2023	5.5	Improper sanitization of incoming intent in Galaxy Store prior to version 4.5.56.6?allows local attackers to access privileged content providers as Galaxy Store permission. **CVE ID : CVE-2023-30705**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	A-SAM-GALA-210823/1517
Product: internet					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 22.0.0.35					
N/A	10-Aug-2023	4.6	Improper Authorization vulnerability in Samsung Internet prior to version 22.0.0.35 allows physical attacker access downloaded files in Secret Mode without user authentication. **CVE ID : CVE-2023-30704**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	A-SAM-INTE-210823/1518
Product: members					
Affected Version(s): * Up to (excluding) 14.0.07.1					
N/A	10-Aug-2023	4.3	Improper URL validation vulnerability in Samsung Members prior to version 14.0.07.1 allows attackers to access sensitive information. **CVE ID : CVE-2023-30703**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	A-SAM-MEMB-210823/1519
Vendor: SAP					
Product: businessobjects_business_intelligence					
Affected Version(s): 420					
Uncontrolled Search Path Element	08-Aug-2023	9	SAP Business Objects Installer - versions 420, 430, allows an authenticated attacker within the network to overwrite an executable file created in a temporary directory during the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installation process. On replacing this executable with a malicious file, an attacker can completely compromise the confidentiality, integrity, and availability of the system **CVE ID : CVE-2023-37490**		
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	4.4	In SAP BusinessObjects Business Intelligence - version 420, If a user logs in to a particular program, under certain specific conditions memory might not be cleared up properly, due to which attacker might be able to get access to user credentials. For a successful attack, the attacker needs to have local access to the system. There is no impact on availability and integrity. **CVE ID : CVE-2023-39440**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1521
Affected Version(s): 430					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	08-Aug-2023	9	SAP Business Objects Installer - versions 420, 430, allows an authenticated attacker within the network to overwrite an executable file created in a temporary directory during the installation process. On replacing this executable with a malicious file, an attacker can completely compromise the confidentiality, integrity, and availability of the system **CVE ID : CVE-2023-37490**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1522
Product: business_one					
Affected Version(s): 10.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	7.5	B1i module of SAP Business One - version 10.0, application allows an authenticated user with deep knowledge to send crafted queries over the network to read or modify the SQL data. On successful exploitation, the attacker can cause high impact on	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability of the application. **CVE ID : CVE-2023-33993**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	SAP business One allows - version 10.0, allows an attacker to insert malicious code into the content of a web page or application and gets it delivered to the client, resulting to Cross-site scripting. This could lead to harmful action affecting the Confidentiality, Integrity and Availability of the application. **CVE ID : CVE-2023-39437**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1524
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.3	SAP Business One (Service Layer) - version 10.0, allows an authenticated attacker with deep knowledge perform certain operation to access unintended data over the network which could lead to high impact on confidentiality	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-210823/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no impact on integrity and availability of the application **CVE ID : CVE-2023-37487**		
Product: commerce_cloud					
Affected Version(s): 2211					
N/A	08-Aug-2023	9.8	SAP Commerce Cloud may accept an empty passphrase for user ID and passphrase authentication, allowing users to log into the system without a passphrase. **CVE ID : CVE-2023-39439**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1526
N/A	08-Aug-2023	7.5	Under certain conditions SAP Commerce (OCC API) - versions HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints allow an attacker to access information which would otherwise be restricted. On successful exploitation there could be a high impact on confidentiality with no impact on	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity and availability of the application. **CVE ID : CVE-2023-37486**		
Product: commerce_hycom					
Affected Version(s): 2105					
N/A	08-Aug-2023	9.8	SAP Commerce Cloud may accept an empty passphrase for user ID and passphrase authentication, allowing users to log into the system without a passphrase. **CVE ID : CVE-2023-39439**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1528
N/A	08-Aug-2023	7.5	Under certain conditions SAP Commerce (OCC API) - versions HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints allow an attacker to access information which would otherwise be restricted. On successful exploitation there could be a high impact on confidentiality with no impact on integrity and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability of the application. **CVE ID : CVE-2023-37486**		
Affected Version(s): 2205					
N/A	08-Aug-2023	9.8	SAP Commerce Cloud may accept an empty passphrase for user ID and passphrase authentication, allowing users to log into the system without a passphrase. **CVE ID : CVE-2023-39439**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1530
N/A	08-Aug-2023	7.5	Under certain conditions SAP Commerce (OCC API) - versions HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints allow an attacker to access information which would otherwise be restricted. On successful exploitation there could be a high impact on confidentiality with no impact on integrity and availability of the application.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-COMM-210823/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37486		
Product: host_agent					
Affected Version(s): 7.22					
Improper Authentication	08-Aug-2023	5.3	Due to missing authentication check in SAP Host Agent - version 7.22, an unauthenticated attacker can set an undocumented parameter to a particular compatibility value and in turn call read functions. This allows the attacker to gather some non-sensitive information about the server. There is no impact on integrity or availability. **CVE ID : CVE-2023-36926**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-210823/1532
Product: message_server					
Affected Version(s): kernel_7.22					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**		
Affected Version(s): kernel_7.53					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**		
Affected Version(s): kernel_7.54					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**		
Affected Version(s): kernel_7.77					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37491		
Affected Version(s): krnl64nuc_7.22					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1537
Affected Version(s): krnl64nuc_7.22ex					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-	A-SAP-MESS-210823/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**	bca6-c68f7e60039b.html	
Affected Version(s): rnl64uc_7.22					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**		
Affected Version(s): rnl64uc_7.22ext					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable. **CVE ID : CVE-2023-37491**		
Affected Version(s): rnl64uc_7.53					
Improper Authorization	08-Aug-2023	8.8	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MESS-210823/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37491		
Product: netweaver_application_server_abap					
Affected Version(s): 700					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37492		
Affected Version(s): 701					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1543
Affected Version(s): 702					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1544
Affected Version(s): 731					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-	A-SAP-NETW-210823/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	bca6-c68f7e60039b.html	
Affected Version(s): 740					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 750					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 752					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 753					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 754					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 755					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37492		
Affected Version(s): 756					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1552
Affected Version(s): 757					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1553
Affected Version(s): 758					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-	A-SAP-NETW-210823/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**	bca6-c68f7e60039b.html	
Affected Version(s): 793					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Affected Version(s): 804					
Missing Authorization	08-Aug-2023	6.5	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack. **CVE ID : CVE-2023-37492**		
Product: netweaver_process_integration					
Affected Version(s): 7.50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	In SAP NetWeaver Process Integration - versions SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50, user-controlled inputs, if not sufficiently encoded, could result in Cross-Site Scripting (XSS) attack. On successful exploitation the attacker can cause limited impact on confidentiality and integrity of the system.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-210823/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37488		
Product: powerdesigner					
Affected Version(s): 16.7					
Improper Access Control	08-Aug-2023	9.8	SAP PowerDesigner - version 16.7, has improper access control which might allow an unauthenticated attacker to run arbitrary queries against the back-end database via Proxy. **CVE ID : CVE-2023-37483**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-POWE-210823/1558
Improper Control of Generation of Code ('Code Injection')	08-Aug-2023	7.8	SAP SQLA for PowerDesigner 17 bundled with SAP PowerDesigner 16.7 SP06 PL03, allows an attacker with local access to the system, to place a malicious library, that can be executed by the application. An attacker could thereby control the behavior of the application. **CVE ID : CVE-2023-36923**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-POWE-210823/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.3	SAP PowerDesigner - version 16.7, queries all password hashes in the backend database and compares it with the user provided one during login attempt, which might allow an attacker to access password hashes from the client's memory. **CVE ID : CVE-2023-37484**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-POWE-210823/1560
Product: supplier_relationship_management					
Affected Version(s): 600					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39436		
Affected Version(s): 602					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1562
Affected Version(s): 603					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**		
Affected Version(s): 604					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1564
Affected Version(s): 605					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-SUPP-210823/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**	c68f7e60039b.html	
Affected Version(s): 606					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1566
Affected Version(s): 616					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM. **CVE ID : CVE-2023-39436**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1567
Affected Version(s): 617					
Exposure of Sensitive Information to an Unauthorized Actor	08-Aug-2023	5.8	SAP Supplier Relationship Management - versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SUPP-210823/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their attacks against SRM. **CVE ID : CVE-2023-39436**		
Vendor: Schneider-electric					
Product: pro-face_gp-pro_ex					
Affected Version(s): * Up to (excluding) 4.09.500					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Aug-2023	5.3	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause memory corruption when an authenticated user opens a tampered log file from GP-Pro EX. **CVE ID : CVE-2023-3953**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-220-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-220-01.pdf	A-SCH-PRO--210823/1569
Vendor: sentry					
Product: sentry					
Affected Version(s): From (including) 22.1.0 Up to (excluding) 23.7.2					
Improper Authentication	07-Aug-2023	8.1	Sentry is an error tracking and performance monitoring platform. Starting in version 22.1.0 and prior to version 23.7.2, an attacker with access to a token with few or no scopes can query `/api/0/api-	https://github.com/getsentry/sentry/pull/53850, https://github.com/getsentry/sentry/commit/fad12c1150d1135edf9666ea72ca11bc110c1083,	A-SEN-SENT-210823/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tokens/` for a list of all tokens created by a user, including tokens with greater scopes, and use those tokens in other requests. There is no evidence that the issue was exploited on `sentry.io`. For self-hosted users, it is advised to rotate user auth tokens. A fix is available in version 23.7.2 of `sentry` and `self-hosted`. There are no known workarounds. **CVE ID : CVE-2023-39349**	https://github.com/getsentry/sentry/security/advisories/GHSA-9jcq-jf57-c62c	
Vendor: sherlock					
Product: gym_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2023	9.8	Code-Projects Gym Management System V1.0 allows remote attackers to execute arbitrary SQL commands via the login form, leading to unauthorized access and potential data manipulation. This vulnerability arises due to insufficient validation of user-supplied input in the username and password fields, enabling SQL Injection attacks.	N/A	A-SHE-GYM_-210823/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37068		
Vendor: Shopex					
Product: ecshop					
Affected Version(s): 4.1.16					
Improper Authentication	04-Aug-2023	6.5	ECShop v4.1.16 contains an arbitrary file deletion vulnerability in the Admin Panel. **CVE ID : CVE-2023-39112**	N/A	A-SHO-ECSH-210823/1572
Vendor: shuize_0x727_project					
Product: shuize_0x727					
Affected Version(s): 1.0					
Improper Control of Generation of Code ('Code Injection')	05-Aug-2023	8.8	ShuiZe_0x727 v1.0 was discovered to contain a remote command execution (RCE) vulnerability via the component /iniFile/config.ini. **CVE ID : CVE-2023-38943**	N/A	A-SHU-SHUI-210823/1573
Vendor: Siemens					
Product: jt2go					
Affected Version(s): * Up to (excluding) 14.2.0.5					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-JT2G-210823/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-JT2G-210823/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38682**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-JT2G-210823/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38683		
Product: jt_open					
Affected Version(s): * Up to (excluding) 11.4					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30795**	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-JT_O-210823/1577
Product: jt_open_toolkit					
Affected Version(s): * Up to (excluding) 11.4					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4). The affected	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-JT_O-210823/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30796**		
Product: jt_utilities					
Affected Version(s): * Up to (excluding) 13.4					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-JT_U-210823/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-30795**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30796**	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-JT_U-210823/1580
Product: parasolid					
Affected Version(s): From (including) 34.0 Up to (excluding) 34.0.253					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-PARA-210823/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30795**		
Affected Version(s): From (including) 34.1 Up to (excluding) 34.1.243					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-PARA-210823/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30795		
Affected Version(s): From (including) 34.1 Up to (excluding) 34.1.258					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38524**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1583
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38527**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38528**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38529**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1588
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Allocation of Resources Without Limits or Throttling	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-38532**		
Affected Version(s): From (including) 35.0 Up to (excluding) 35.0.177					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30795**	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-PARA-210823/1592
Affected Version(s): From (including) 35.0 Up to (excluding) 35.0.254					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions <	https://cert-portal.siemens.com/produc	A-SIE-PARA-210823/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38524**	tcert/pdf/ssa-407785.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38527**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38528**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1597
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38529**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Allocation of Resources Without Limits or Throttling	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition.	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38532		
Affected Version(s): From (including) 35.1 Up to (excluding) 35.1.073					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-30795**	https://cert-portal.siemens.com/productcert/pdf/ssa-001569.pdf	A-SIE-PARA-210823/1602
Affected Version(s): From (including) 35.1 Up to (excluding) 35.1.171					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38524**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1606
Allocation of Resources	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All	https://cert-portal.siemens.com/produc	A-SIE-PARA-210823/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-38532**	tcert/pdf/ssa-407785.pdf	
Affected Version(s): From (including) 35.1 Up to (excluding) 35.1.184					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38529**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Affected Version(s): From (including) 35.1 Up to (excluding) 35.1.197					
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an allocated buffer	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-PARA-210823/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38528**		
Product: ruggedcom_crossbow					
Affected Version(s): * Up to (excluding) 5.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	9.8	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an unauthenticated remote attackers to execute arbitrary SQL queries on the server database. **CVE ID : CVE-2023-37372**	https://cert-portal.siemens.com/productcert/pdf/ssa-472630.pdf	A-SIE-RUGG-210823/1611
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2023	8.8	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an authenticated remote attackers to execute arbitrary SQL queries on the server database and escalate privileges.	https://cert-portal.siemens.com/productcert/pdf/ssa-472630.pdf	A-SIE-RUGG-210823/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27411		
Missing Authentication for Critical Function	08-Aug-2023	7.5	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications accept unauthenticated file write messages. An unauthenticated remote attacker could write arbitrary files to the affected application's file system. **CVE ID : CVE-2023-37373**	https://cert-portal.siemens.com/productcert/pdf/ssa-472630.pdf	A-SIE-RUGG-210823/1613
Product: sicam_toolbox_ii					
Affected Version(s): * Up to (excluding) 07.10					
N/A	08-Aug-2023	7.8	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). The affected application's database service is executed as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges. **CVE ID : CVE-2023-38641**	https://cert-portal.siemens.com/productcert/pdf/ssa-975961.pdf	A-SIE-SICA-210823/1614
Product: solid_edge					
Affected Version(s): * Up to (excluding) se2023					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39181**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1615
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39182**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1616
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7).	https://cert-portal.siemens.com/produc	A-SIE-SOLI-210823/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39183**	tcert/pdf/ssa-811403.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39184**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1618
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39185**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39186**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1620
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-39187**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39188**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1622
Affected Version(s): se2023					
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39181		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39182**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1624
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39183**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39184**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1626
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39185**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1627
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7).	https://cert-portal.siemens.com/produc	A-SIE-SOLI-210823/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39186**	tcert/pdf/ssa-811403.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39187**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1629
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39188**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-39419**	https://cert-portal.siemens.com/productcert/pdf/ssa-811403.pdf	A-SIE-SOLI-210823/1631
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 2). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted DWG file. An attacker could leverage this vulnerability to	https://cert-portal.siemens.com/productcert/pdf/ssa-932528.pdf	A-SIE-SOLI-210823/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. (ZDI-CAN-19562) **CVE ID : CVE-2023-39549**		
Product: solid_edge_se2022					
Affected Version(s): -					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_1					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_10					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_11					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_12					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_2					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_3					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_4					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_5					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_7					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_8					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): maintenance_pack_9					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Product: solid_edge_se2023					
Affected Version(s): -					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): update_0001					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): update_0002					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): update_0003					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-SOLI-210823/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-28830**		
Product: teamcenter_visualization					
Affected Version(s): 14.1					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38524**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1649
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions <	https://cert-portal.siemens.com/produc	A-SIE-TEAM-210823/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**	tcert/pdf/ssa-407785.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38527**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-38528**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38529**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1654
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258),	https://cert-portal.siemens.com/produc	A-SIE-TEAM-210823/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**	tcert/pdf/ssa-407785.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Allocation of Resources Without Limits or Throttling	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-38532**		
Affected Version(s): 14.3					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38524		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1659
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38527**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38528**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38529		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1664
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Allocation of Resources Without Limits or Throttling	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-38532**		
Affected Version(s): From (including) 13.2.0 Up to (excluding) 13.2.0.15					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): From (including) 13.3.0 Up to (excluding) 13.3.0.11					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.0.10					
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38682		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38683**	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1670
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.0.11					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4),	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.0.5					
Use After Free	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-28830**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V14.2 (All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38682**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-131450.pdf	A-SIE-TEAM-210823/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-38683**		
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.0.6					
NULL Pointer Dereference	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38524**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1675
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38525**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38526**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38527**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. **CVE ID : CVE-2023-38528**		
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38529**	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1680
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258),	https://cert-portal.siemens.com/produc	A-SIE-TEAM-210823/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38530**	tcert/pdf/ssa-407785.pdf	
Out-of-bounds Read	08-Aug-2023	7.8	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-38531**		
Allocation of Resources Without Limits or Throttling	08-Aug-2023	5.5	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack	https://cert-portal.siemens.com/productcert/pdf/ssa-407785.pdf	A-SIE-TEAM-210823/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-38532**		
Product: tecnomatix					
Affected Version(s): From (including) 2201 Up to (excluding) 2201.0008					
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21106) **CVE ID : CVE-2023-38679**	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1684
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21132) **CVE ID : CVE-2023-38680**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21270)	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38681		
Affected Version(s): From (including) 2302 Up to (excluding) 2302.0002					
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21106) **CVE ID : CVE-2023-38679**	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1687
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21132) **CVE ID : CVE-2023-38680**		
Out-of-bounds Write	08-Aug-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21270) **CVE ID : CVE-2023-38681**	https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf	A-SIE-TECN-210823/1689
Vendor: Silverstripe					
Product: framework					
Affected Version(s): * Up to (excluding) 4.3.14					
Improper Input Validation	01-Aug-2023	8.1	Silverstripe Framework is the MVC framework that powers Silverstripe	https://github.com/silverstripe/silverstripe-	A-SIL-FRAM-210823/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CMS. When a new member record is created and a password is not set, an empty encrypted password is generated. As a result, if someone is aware of the existence of a member record associated with a specific email address, they can potentially attempt to log in using that empty password. Although the default member authenticator and login form require a non-empty password, alternative authentication methods might still permit a successful login with the empty password. This issue has been patched in versions 4.13.4 and 5.0.13. **CVE ID : CVE-2023-32302**	framework/commit/7b21b38ac4532d06565dfcefad50540ebd2b50f4, https://github.com/silverstripe/silverstripe-framework/security/advisories/GHSA-36xx-7vf6-7mv3	
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.13					
Improper Input Validation	01-Aug-2023	8.1	Silverstripe Framework is the MVC framework that powers Silverstripe	https://github.com/silverstripe/silverstripe-	A-SIL-FRAM-210823/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CMS. When a new member record is created and a password is not set, an empty encrypted password is generated. As a result, if someone is aware of the existence of a member record associated with a specific email address, they can potentially attempt to log in using that empty password. Although the default member authenticator and login form require a non-empty password, alternative authentication methods might still permit a successful login with the empty password. This issue has been patched in versions 4.13.4 and 5.0.13. **CVE ID : CVE-2023-32302**	framework/commit/7b21b38ac4532d06565dfcefad50540ebd2b50f4, https://github.com/silverstripe/silverstripe-framework/security/advisories/GHSA-36xx-7vf6-7mv3	
Vendor: simonsmith					
Product: cypress_image_snapshot					
Affected Version(s): * Up to (excluding) 8.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2023	6.5	cypress-image-snapshot shows visual regressions in Cypress with jest-image-snapshot. Prior to version 8.0.2, it's possible for a user to pass a relative file path for the snapshot name and reach outside of the project directory into the machine running the test. This issue has been patched in version 8.0.2. **CVE ID : CVE-2023-38695**	https://github.com/simonsmith/cypress-image-snapshot/commit/ef49519795daf5183f4fac6f3136e194f20f39f4, https://github.com/simonsmith/cypress-image-snapshot/security/advisories/GHSA-vxjg-hchx-cc4g	A-SIM-CYPR-210823/1692
Vendor: simplecoding					
Product: terms_descriptions					
Affected Version(s): * Up to (including) 3.4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Vladimir Statsenko Terms descriptions plugin <= 3.4.4 versions. **CVE ID : CVE-2023-28779**	N/A	A-SIM-TERM-210823/1693
Vendor: Smackcoders					
Product: wp_ultimate_csv_importer					
Affected Version(s): * Up to (including) 7.9.8					
Improper Privilege	04-Aug-2023	8.8	The WP Ultimate CSV Importer plugin for WordPress is	https://plugins.trac.wordpress.org/change	A-SMA-WP_U-210823/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			vulnerable to privilege escalation in versions up to, and including, 7.9.8 due to insufficient restriction on the 'get_header_values' function. This makes it possible for authenticated attackers, with minimal permissions such as an author, if the administrator previously grants access in the plugin settings, to modify their user role by supplying the 'wp_capabilities->cus1' parameter. **CVE ID : CVE-2023-4140**	set/2944635/wp-ultimate-csv-importer/trunk/wp-ultimate-csv-importer.php	
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	8.8	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 7.9.8 via the '->cus2' parameter. This allows authenticated attackers with author-level permissions or above, if the administrator previously grants access in the plugin settings, to create a PHP file and execute	https://plugins.trac.wordpress.org/changeset/2944635/wp-ultimate-csv-importer/trunk/wp-ultimate-csv-importer.php	A-SMA-WP_U-210823/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code on the server. The author resolved this vulnerability by removing the ability for authors and editors to import files, please note that this means php file creation is still allowed for site administrators, use the plugin with caution. **CVE ID : CVE-2023-4141**		
Improper Control of Generation of Code ('Code Injection')	04-Aug-2023	8.8	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 7.9.8 via the '->cus1' parameter. This allows authenticated attackers with author-level permissions or above, if the administrator previously grants access in the plugin settings, to execute code on the server. The author resolved this vulnerability by removing the ability for authors and editors to import files, please note that this means remote code execution is still	https://plugins.trac.wordpress.org/changeset/2944635/wp-ultimate-csv-importer/trunk/wp-ultimate-csv-importer.php	A-SMA-WP_U-210823/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for site administrators, use the plugin with caution. **CVE ID : CVE-2023-4142**		
Exposure of Sensitive Information to an Unauthorized Actor	04-Aug-2023	7.5	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Sensitive Information Exposure via Directory Listing due to missing restriction in export folder indexing in versions up to, and including, 7.9.8. This makes it possible for unauthenticated attackers to list and view exported files. **CVE ID : CVE-2023-4139**	https://plugins.trac.wordpress.org/changeset/2944635/wp-ultimate-csv-importer/trunk/wp-ultimate-csv-importer.php	A-SMA-WP_U-210823/1697
Vendor: socketry					
Product: protocol-http1					
Affected Version(s): * Up to (excluding) 0.15.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	protocol-http1 provides a low-level implementation of the HTTP/1 protocol. RFC 9112 Section 7.1 defined the format of chunk size, chunk data and chunk extension. The value of Content-Length header should be a string of 0-9 digits, the chunk size should be a string of	https://github.com/socketry/protocol-http1/security/advisories/GHSA-6jwc-qr2q-7xwj, https://github.com/socketry/protocol-http1/commit/e11fc164fd2b36f7b7e785e	A-SOC-PROT-210823/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hex digits and should split from chunk data using CRLF, and the chunk extension shouldn't contain any invisible character. However, Falcon has following behaviors while disobey the corresponding RFCs: accepting Content-Length header values that have `+` prefix, accepting Content-Length header values that written in hexadecimal with `0x` prefix, accepting `0x` and `+` prefixed chunk size, and accepting LF in chunk extension. This behavior can lead to desync when forwarding through multiple HTTP parsers, potentially results in HTTP request smuggling and firewall bypassing. This issue is fixed in `protocol-http1` v0.15.1. There are no known workarounds. **CVE ID : CVE-2023-38697**	69fa8859eb06bcedd	
Vendor: spidercontrol					
Product: scadawebserver					
Affected Version(s): * Up to (including) 2.08					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2023	6.5	SpiderControl SCADA Webserver versions 2.08 and prior are vulnerable to path traversal. An attacker with administrative privileges could overwrite files on the webserver using the HMI's upload file feature. This could create size zero files anywhere on the webserver, potentially overwriting system files and creating a denial-of-service condition. **CVE ID : CVE-2023-3329**	N/A	A-SPI-SCAD-210823/1699
Vendor: spiderteams					
Product: applyonline_-_application_form_builder_and_manager					
Affected Version(s): * Up to (including) 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Spider Teams ApplyOnline plugin <= 2.5 versions. **CVE ID : CVE-2023-24391**	N/A	A-SPI-APPL-210823/1700
Vendor: sulu					
Product: sulu					
Affected Version(s): From (including) 2.5.0 Up to (excluding) 2.5.10					
Observable Response	04-Aug-2023	4.3	Sulu is an open-source PHP content management system based on the	https://github.com/sulu/sulu/commit/5f6c98ba030b20	A-SUL-SULU-210823/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Discrepancy			Symfony framework. It allows over the Admin Login form to detect which user (username, email) exists and which one do not exist. Sulu Installation not using the old Symfony 5.4 security System and previous version are not impacted by this Security issue. The vulnerability has been patched in version 2.5.10. **CVE ID : CVE-2023-39343**	05793e2dc647cc938937ea889b, https://github.com/sulu/sulu/security/advisories/GHSA-wmwf-49vv-p3mr	
Vendor: supito					
Product: mahato_simple_light_weight_social_share					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sudipto Pratap Mahato Simple Light Weight Social Share plugin <= 2.0 versions. **CVE ID : CVE-2023-37388**	N/A	A-SUP-MAHA-210823/1702
Vendor: supremainc					
Product: biostar_2					
Affected Version(s): * Up to (excluding) 2.9.1					
Improper Neutralization of	03-Aug-2023	8.8	An OS Command injection vulnerability exists	https://kb.supremainc.com/knowledge/d	A-SUP-BIOS-220823/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in Suprema BioStar 2 before V2.9.1, which allows authenticated users to execute arbitrary OS commands on the BioStar 2 server. **CVE ID : CVE-2023-33364**	oku.php?id=en:release_note_291	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	8.8	A SQL injection vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows authenticated users to inject arbitrary SQL directives into an SQL statement and execute arbitrary SQL commands. **CVE ID : CVE-2023-33366**	N/A	A-SUP-BIOS-220823/1704
Improper Authentication	03-Aug-2023	7.5	An authentication bypass vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows unauthenticated users to access some functionality on BioStar 2 servers. **CVE ID : CVE-2023-33363**	https://kb.supremainc.com/knowledge/doku.php?id=en:release_note_291	A-SUP-BIOS-220823/1705
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.5	A path traversal vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows unauthenticated attackers to fetch arbitrary files from	https://kb.supremainc.com/knowledge/doku.php?id=en:release_note_291	A-SUP-BIOS-220823/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the server's web server. **CVE ID : CVE-2023-33365**		
Vendor: syntacticsinc					
Product: easync					
Affected Version(s): * Up to (including) 1.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Syntactics, Inc. EaSYNC plugin <= 1.3.7 versions. **CVE ID : CVE-2023-38384**	N/A	A-SYN-EASY-220823/1707
Vendor: te-st					
Product: leyka					
Affected Version(s): * Up to (including) 3.30.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.30.2 versions. **CVE ID : CVE-2023-39314**	N/A	A-TE--LEYK-220823/1708
Vendor: tel-ster					
Product: telwin_scada_webinterface					
Affected Version(s): 9.0					
Improper Limitation of a Pathname to a Restricted Directory	03-Aug-2023	7.5	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly	https://www.tel-ster.pl/index.php/telwin-scada/nowosci/372-telwin-scada-podatnosc-	A-TEL-TELW-220823/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system. **CVE ID : CVE-2023-0956**	cve-2023-0956	
Affected Version(s): 8.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.5	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system. **CVE ID : CVE-2023-0956**	https://www.tel-ster.pl/index.php/telwin-scada/nowosci/372-telwin-scada-podatnosc-cve-2023-0956	A-TEL-TELW-220823/1710
Affected Version(s): From (including) 3.2 Up to (excluding) 6.2					
Improper Limitation of a Pathname to a Restricted Directory	03-Aug-2023	7.5	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly	https://www.tel-ster.pl/index.php/telwin-scada/nowosci/372-telwin-scada-podatnosc-	A-TEL-TELW-220823/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system. **CVE ID : CVE-2023-0956**	cve-2023-0956	
Affected Version(s): From (including) 7.0 Up to (excluding) 7.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.5	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system. **CVE ID : CVE-2023-0956**	https://www.tel-ster.pl/index.php/telwin-scada/nowosci/372-telwin-scada-podatnosc-cve-2023-0956	A-TEL-TELW-220823/1712
Vendor: templatecookie					
Product: adlisting					
Affected Version(s): 2.14.0					
N/A	05-Aug-2023	7.5	A vulnerability was found in Templatecookie Adlisting 2.14.0. It has been classified as problematic.	N/A	A-TEM-ADLI-220823/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected is an unknown function of the file /ad-list of the component Redirect Handler. The manipulation leads to information disclosure. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-236184. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4168**		
Vendor: Textpattern					
Product: textpattern					
Affected Version(s): 4.8.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Aug-2023	7.2	Directory Traversal vulnerability in Textpattern CMS v4.8.8 allows a remote authenticated attacker to execute arbitrary code and gain access to sensitive information via the plugin Upload function. **CVE ID : CVE-2023-36220**	N/A	A-TEX-TEXT-220823/1714
Vendor: themeqx					
Product: letterpress					
Affected Version(s): * Up to (including) 1.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themeqx LetterPress plugin <= 1.1.2 versions. **CVE ID : CVE-2023-27415**	N/A	A-THE-LETT-220823/1715
Vendor: toll_tax_management_system_project					
Product: toll_tax_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2023	6.1	Cross Site Scripting (XSS) vulnerability in sourcecodester Toll Tax Management System 1.0 allows remote attackers to run arbitrary code via the First Name and Last Name fields on the My Account page. **CVE ID : CVE-2023-36158**	N/A	A-TOL-TOLL-220823/1716
Vendor: tongda2000					
Product: tongda_oa					
Affected Version(s): 11.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2023	9.8	A vulnerability, which was classified as critical, was found in Tongda OA. This affects an unknown part of the file general/system/seal_manage/iweboffice/delete_seal.php. The manipulation of the argument DELETE_STR leads to sql injection. The	N/A	A-TON-TONG-220823/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-236181 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4165**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2023	9.8	A vulnerability has been found in Tongda OA and classified as critical. This vulnerability affects unknown code of the file general/system/seal_manage/dianju/delete_log.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-	N/A	A-TON-TONG-220823/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			236182 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4166**		
Vendor: totalcms					
Product: total_cms					
Affected Version(s): 1.7.4					
Unrestricted Upload of File with Dangerous Type	03-Aug-2023	8.8	File Upload vulnerability in Total CMS v.1.7.4 allows a remote attacker to execute arbitrary code via a crafted PHP file to the edit page function. **CVE ID : CVE-2023-36212**	N/A	A-TOT-TOTA-220823/1719
Vendor: tribe29					
Product: checkmk					
Affected Version(s): * Up to (including) 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	Reflected XSS in business intelligence in Checkmk <2.2.0p8, <2.1.0p32, <2.0.0p38, <=1.6.0p30. **CVE ID : CVE-2023-23548**	https://checkmk.com/werk/15691	A-TRI-CHEC-220823/1720
Affected Version(s): 2.0.0					
Improper Neutralization of Input	01-Aug-2023	6.1	Reflected XSS in business intelligence in Checkmk <2.2.0p8, <2.1.0p32,	https://checkmk.com/werk/15691	A-TRI-CHEC-220823/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			<2.0.0p38, <=1.6.0p30. **CVE ID : CVE-2023-23548**		
Affected Version(s): 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	Reflected XSS in business intelligence in Checkmk <2.2.0p8, <2.1.0p32, <2.0.0p38, <=1.6.0p30. **CVE ID : CVE-2023-23548**	https://checkmk.com/werk/15691	A-TRI-CHEC-220823/1722
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2023	6.1	Reflected XSS in business intelligence in Checkmk <2.2.0p8, <2.1.0p32, <2.0.0p38, <=1.6.0p30. **CVE ID : CVE-2023-23548**	https://checkmk.com/werk/15691	A-TRI-CHEC-220823/1723
Vendor: typecho					
Product: typecho					
Affected Version(s): 1.2.1					
Unrestricted Upload of File with Dangerous Type	03-Aug-2023	8.8	A File Upload vulnerability in typecho v.1.2.1 allows a remote attacker to execute arbitrary code via the upload and options-general parameters in index.php. **CVE ID : CVE-2023-36299**	https://github.com/typecho/typecho/releases/tag/v1.2.1, https://github.com/MentalityXt/typecho-v1.2.1-RCE	A-TYP-TYPE-220823/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: verint					
Product: engagement_management					
Affected Version(s): 15.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	Verint Engagement Management 15.3 Update 2023R2 is vulnerable to HTML injection via the user data form in the live chat. **CVE ID : CVE-2023-33257**	N/A	A-VER-ENGA-220823/1725
Vendor: viatomtech					
Product: vihealth					
Affected Version(s): * Up to (including) 2.74.58					
N/A	01-Aug-2023	7.8	An issue in Viatom Health ViHealth for Android v.2.74.58 and before allows a remote attacker to execute arbitrary code via the com.viatom.baselib.mvvm.webWebView Activity component. **CVE ID : CVE-2023-36351**	N/A	A-VIA-VIHE-220823/1726
Vendor: villatheme					
Product: wpbulky					
Affected Version(s): * Up to (excluding) 1.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in VillaTheme WPBulky plugin <= 1.0.10 versions. **CVE ID : CVE-2023-30482**	N/A	A-VIL-WPBU-220823/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: VIM					
Product: vim					
Affected Version(s): 9.0.1367					
Divide By Zero	07-Aug-2023	7.8	Divide By Zero in vim/vim from 9.0.1367-1 to 9.0.1367-3 **CVE ID : CVE-2023-3896**	https://github.com/vim/vim/pull/12540, https://github.com/vim/vim/issues/12528	A-VIM-VIM-220823/1728
Vendor: Vmware					
Product: horizon_client					
Affected Version(s): 2006					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1729
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration.	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34038		
Affected Version(s): 2012					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1731
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1732
Affected Version(s): 2103					
Inconsistent Interpretation of	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling	https://www.vmware.com/security/advisories/VMSA-	A-VMW-HORI-220823/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
HTTP Requests ('HTTP Request Smuggling')			vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	2023-0017.html	
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1734
Affected Version(s): 2106					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests.	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34037		
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1736
Affected Version(s): 2111					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1737
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information relating to the internal network configuration. **CVE ID : CVE-2023-34038**		
Affected Version(s): 2111.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1739
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2203					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE ID : CVE-2023-34037**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1741
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1742
Affected Version(s): 2212					
Inconsistent Interpretation of HTTP Requests ('HTTP Request	04-Aug-2023	5.3	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Smuggling')			HTTP smuggle requests. **CVE ID : CVE-2023-34037**		
N/A	04-Aug-2023	5.3	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration. **CVE ID : CVE-2023-34038**	https://www.vmware.com/security/advisories/VMSA-2023-0017.html	A-VMW-HORI-220823/1744
Vendor: vyperlang					
Product: vyper					
Affected Version(s): 0.2.15					
Incorrect Authorization	07-Aug-2023	5.9	Vyer is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). In versions 0.2.15, 0.2.16 and 0.3.0, named re-entrancy locks are allocated incorrectly. Each function using a named re-entrancy lock gets a unique lock regardless of the key, allowing cross-	https://github.com/vyperlang/vyper/security/advisories/GHSA-5824-cm3x-3c38, https://github.com/vyperlang/vyper/pull/2514, https://github.com/vyperlang/vyper/pull/2439	A-VYP-VYPE-220823/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function re-entrancy in contracts compiled with the susceptible versions. A specific set of conditions is required to result in misbehavior of affected contracts, specifically: a `.vy` contract compiled with `vyper` versions `0.2.15`, `0.2.16`, or `0.3.0`; a primary function that utilizes the `@nonreentrant` decorator with a specific `key` and does not strictly follow the check-effects-interaction pattern (i.e. contains an external call to an untrusted party before storage updates); and a secondary function that utilizes the same `key` and would be affected by the improper state caused by the primary function. Version 0.3.1 contains a fix for this issue. **CVE ID : CVE-2023-39363**		
Affected Version(s): 0.2.16					
Incorrect Authorization	07-Aug-2023	5.9	Vyer is a Pythonic Smart Contract Language for the Ethereum Virtual	https://github.com/vyperlang/vyper/security/advisori	A-VYP-VYPE-220823/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Machine (EVM). In versions 0.2.15, 0.2.16 and 0.3.0, named re-entrancy locks are allocated incorrectly. Each function using a named re-entrancy lock gets a unique lock regardless of the key, allowing cross-function re-entrancy in contracts compiled with the susceptible versions. A specific set of conditions is required to result in misbehavior of affected contracts, specifically: a `.vy` contract compiled with `vyper` versions `0.2.15`, `0.2.16`, or `0.3.0`; a primary function that utilizes the `@nonreentrant` decorator with a specific `key` and does not strictly follow the check-effects-interaction pattern (i.e. contains an external call to an untrusted party before storage updates); and a secondary function that utilizes the same `key` and would be affected by the improper state caused by the primary function.	es/GHSA-5824-cm3x-3c38, https://github.com/vyperlang/vyper/pull/2514, https://github.com/vyperlang/vyper/pull/2439	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version 0.3.1 contains a fix for this issue. **CVE ID : CVE-2023-39363**		
Affected Version(s): 0.3.0					
Incorrect Authorization	07-Aug-2023	5.9	Vyer is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). In versions 0.2.15, 0.2.16 and 0.3.0, named re-entrancy locks are allocated incorrectly. Each function using a named re-entrancy lock gets a unique lock regardless of the key, allowing cross-function re-entrancy in contracts compiled with the susceptible versions. A specific set of conditions is required to result in misbehavior of affected contracts, specifically: a `.vy` contract compiled with `vyper` versions `0.2.15`, `0.2.16`, or `0.3.0`; a primary function that utilizes the `@nonreentrant` decorator with a specific `key` and does not strictly follow the check-effects-interaction pattern (i.e. contains	https://github.com/vyperlang/vyper/security/advisories/GHSA-5824-cm3x-3c38, https://github.com/vyperlang/vyper/pull/2514, https://github.com/vyperlang/vyper/pull/2439	A-VYP-VYPE-220823/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an external call to an untrusted party before storage updates); and a secondary function that utilizes the same `key` and would be affected by the improper state caused by the primary function. Version 0.3.1 contains a fix for this issue. **CVE ID : CVE-2023-39363**		
Vendor: Wbce					
Product: wbce_cms					
Affected Version(s): 1.6.1					
Unrestricted Upload of File with Dangerous Type	03-Aug-2023	7.2	An arbitrary file upload vulnerability in the /languages/install.php component of WBCE CMS v1.6.1 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-38947**	N/A	A-WBC-WBCE-220823/1748
Vendor: web-settler					
Product: layer_slider					
Affected Version(s): * Up to (including) 1.1.9.7					
Improper Neutralization of Input During Web Page Generation	10-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Muneeb Layer Slider	N/A	A-WEB-LAYE-220823/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 1.1.9.7 versions. **CVE ID : CVE-2023-23798**		
Vendor: webboss					
Product: webboss.io_cms					
Affected Version(s): 3.7.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	5.4	WebBoss.io CMS v3.7.0.1 contains a stored Cross-Site Scripting (XSS) vulnerability due to lack of input validation and output encoding. **CVE ID : CVE-2023-39096**	N/A	A-WEB-WEBB-220823/1750
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	5.4	WebBoss.io CMS v3.7.0.1 contains a stored cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2023-39097**	N/A	A-WEB-WEBB-220823/1751
Vendor: webcodingplace					
Product: real_estate_manager					
Affected Version(s): * Up to (including) 6.7.1					
Improper Privilege Management	09-Aug-2023	6.5	The Real Estate Manager plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 6.7.1 due to insufficient restriction on the 'rem_save_profile_front' function. This	N/A	A-WEB-REAL-220823/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_capabilities' parameter during a profile update. **CVE ID : CVE-2023-4239**		
Vendor: webdzier					
Product: button					
Affected Version(s): * Up to (including) 1.1.23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Webdzier Button plugin <= 1.1.23 versions. **CVE ID : CVE-2023-23871**	N/A	A-WEB-BUTT-220823/1753
Vendor: Webkul					
Product: uvdesk					
Affected Version(s): 1.1.3					
Unrestricted Upload of File with Dangerous Type	01-Aug-2023	7.8	An arbitrary file upload vulnerability in Uvdesk 1.1.3 allows attackers to execute arbitrary code via uploading a crafted image file. **CVE ID : CVE-2023-39147**	N/A	A-WEB-UVDE-220823/1754
Vendor: webmechanix					
Product: add_posts_to_pages					
Affected Version(s): * Up to (including) 1.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Arsham Mirshah Add Posts to Pages plugin <= 1.4.1 versions. **CVE ID : CVE-2023-23826**	N/A	A-WEB-ADD_-220823/1755
Vendor: wger					
Product: workout_manager					
Affected Version(s): 2.2.0					
Cross-Site Request Forgery (CSRF)	08-Aug-2023	8.8	Cross Site Request Forgery (CSRF) vulnerability in wger Project wger Workout Manager 2.2.0a3 allows a remote attacker to gain privileges via the user-management feature in the gym/views/gym.py, templates/gym/reset_user_password.html, templates/user/overview.html, core/views/user.py, and templates/user/preferences.html, core/forms.py components. **CVE ID : CVE-2023-38759**	N/A	A-WGE-WORK-220823/1756
Improper Neutralization of Input During	08-Aug-2023	5.4	Cross Site Scripting vulnerability in wger Project wger Workout Manager v.2.2.0a3 allows a	N/A	A-WGE-WORK-220823/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			remote attacker to gain privileges via the license_author field in the add-ingredient function in the templates/ingredients/view.html, models/ingredients.py, and views/ingredients.py components. **CVE ID : CVE-2023-38758**		
Vendor: winitor					
Product: pestudio					
Affected Version(s): 9.52					
Uncontrolled Search Path Element	08-Aug-2023	7.8	An issue in PEStudio v.9.52 allows a remote attacker to execute arbitrary code via a crafted DLL file to the PESstudio exeutable. **CVE ID : CVE-2023-36546**	N/A	A-WIN-PEST-220823/1758
Vendor: Woocommerce					
Product: shipping_multiple_addresses					
Affected Version(s): * Up to (including) 3.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Shipping Multiple Addresses plugin <= 3.8.5 versions. **CVE ID : CVE-2023-37873**	N/A	A-WOO-SHIP-220823/1759
Vendor: wow-company					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bubble_menu					
Affected Version(s): * Up to (excluding) 3.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	4.8	The Bubble Menu WordPress plugin before 3.0.5 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup). **CVE ID : CVE-2023-3650**	N/A	A-WOW-BUBB-220823/1760
Vendor: wp-buy					
Product: wp_content_copy_protection_\&_no_right_click					
Affected Version(s): * Up to (including) 3.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP-buy WP Content Copy Protection & No Right Click plugin <= 3.5.5 versions. **CVE ID : CVE-2023-36678**	N/A	A-WP--WP_C-220823/1761
Vendor: wp-cirrus_project					
Product: wp-cirrus					
Affected Version(s): * Up to (including) 0.6.11					
Improper Neutralization of Input	08-Aug-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-WP--WP-C-220823/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Christian Kramer & Hendrik Thole WP-Cirrus plugin <= 0.6.11 versions. **CVE ID : CVE-2023-36692**		
Vendor: wpazure					
Product: upfrontwp					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	5.4	Auth. (subscriber+) Reflected Cross-site Scripting (XSS) vulnerability in Wpazure Themes Upfrontwp theme <= 1.1 versions. **CVE ID : CVE-2023-24009**	N/A	A-WPA-UPFR-220823/1763
Vendor: wpcode					
Product: wpcode					
Affected Version(s): * Up to (including) 2.0.13.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	6.1	The WPCode WordPress plugin before 2.0.13.1 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2023-3524**	N/A	A-WPC-WPCO-220823/1764
Vendor: wpdeveloper					
Product: embedpress					
Affected Version(s): * Up to (including) 3.8.2					
Improper Neutralization of Input	10-Aug-2023	5.4	The EmbedPress plugin for WordPress is vulnerable to Stored	https://plugins.trac.wordpress.org/changeset/2950211/	A-WPD-EMBE-220823/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting via the 'embedpress_calendar' shortcode in versions up to, and including, 3.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-4283**	embedpress#file18, https://plugins.trac.wordpress.org/browser/embedpress/tags/3.8.2/EmbedPress/ThirdParty/Googlecalendar/Embedpress_Google_Helper.php#L522	
Missing Authorization	10-Aug-2023	4.3	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'admin_post_remove' and 'remove_private_data' functions in versions up to, and including, 3.8.2. This makes it possible for authenticated attackers with subscriber privileges	https://plugins.trac.wordpress.org/changeset/2950211/embedpress#file18, https://plugins.trac.wordpress.org/browser/embedpress/tags/3.8.2/EmbedPress/ThirdParty/Googlecalendar/Embedpress_Google_Helper.php#L801	A-WPD-EMBE-220823/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or above, to delete plugin settings. **CVE ID : CVE-2023-4282**		
Vendor: wpfactory					
Product: wpfactory_helper					
Affected Version(s): * Up to (including) 1.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPFactory WPFactory Helper plugin <= 1.5.2 versions. **CVE ID : CVE-2023-36689**	N/A	A-WPF-WPFA-220823/1767
Vendor: wpfoodmanager					
Product: wp_food_manager					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	5.4	The WP Food Manager WordPress plugin before 1.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-0604**	N/A	A-WPF-WP_F-220823/1768
Vendor: wpgogo					
Product: custom_field_template					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Hiroaki Miyashita Custom Field Template plugin <= 2.5.9 versions. **CVE ID : CVE-2023-38392**	N/A	A-WPG-CUST-220823/1769
Vendor: ws-inc					
Product: j_wbem					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.7.5					
Improper Restriction of XML External Entity Reference	03-Aug-2023	9.1	In WS-Inc J WBEM Server 4.7.4 before 4.7.5, the CIM-XML protocol adapter does not disable entity resolution. This allows context-dependent attackers to read arbitrary files or cause a denial of service, a similar issue to CVE-2013-4152. **CVE ID : CVE-2023-37364**	https://ws-inc.com/security.html	A-WS--J_WB-220823/1770
Vendor: xithrius					
Product: twitch-tui					
Affected Version(s): * Up to (including) 2.4.0					
Missing Encryption of Sensitive Data	04-Aug-2023	7.5	twitch-tui provides Twitch chat in a terminal. Prior to version 2.4.1, the connection is not using TLS for communication. In the configuration of the irc connection,	https://github.com/Xithrius/twitch-tui/commit/74d13ddca35f8f0816f4933c229da1fd95c0350a, https://github	A-XIT-TWIT-220823/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the software disables TLS, which makes all communication to Twitch IRC servers unencrypted. As a result, communication, including auth tokens, can be sniffed. Version 2.4.1 has a patch for this issue. **CVE ID : CVE-2023-38688**	.com/Xithrius/twitch-tui/security/advisories/GHSA-779w-xvpm-78jx	
Vendor: Xoops					
Product: xoops					
Affected Version(s): 2.5.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	9	Cross Site Scripting vulnerability in Xoops CMS v.2.5.10 allows a remote attacker to execute arbitrary code via the category name field of the image manager function. **CVE ID : CVE-2023-36217**	N/A	A-XOO-XOOP-220823/1772
Vendor: yikesinc					
Product: easy_forms_for_mailchimp					
Affected Version(s): * Up to (including) 6.8.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in YIKES, Inc. Easy Forms for Mailchimp plugin <= 6.8.8 versions. **CVE ID : CVE-2023-23900**	N/A	A-YIK-EASY-220823/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Zabbix					
Product: frontend					
Affected Version(s): * Up to (excluding) 6.225.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A security defect was identified in Foundry Frontend that enabled users to potentially conduct DOM XSS attacks if Foundry's CSP were to be bypassed. This defect was resolved with the release of Foundry Frontend 6.225.0. **CVE ID : CVE-2023-30958**	https://palantir.safebase.us/?tcuUid=5764b094-d3c0-4380-90f2-234f36116c9b	A-ZAB-FRON-220823/1774
Vendor: zkteco					
Product: bioaccess_ivs					
Affected Version(s): 3.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2023	9.8	ZKTeco BioAccess IVS v3.3.1 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2023-38954**	N/A	A-ZKT-BIOA-220823/1775
Exposure of Resource to Wrong Sphere	03-Aug-2023	7.5	ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to obtain sensitive information about all managed devices, including	N/A	A-ZKT-BIOA-220823/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP addresses and device names. **CVE ID : CVE-2023-38955**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.5	A path traversal vulnerability in ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to read arbitrary files via supplying a crafted payload. **CVE ID : CVE-2023-38956**	N/A	A-ZKT-BIOA-220823/1777
Incorrect Authorization	03-Aug-2023	5.3	An access control issue in ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to arbitrarily close and open the doors managed by the platform remotely via sending a crafted web request. **CVE ID : CVE-2023-38958**	N/A	A-ZKT-BIOA-220823/1778
Product: biotime					
Affected Version(s): 8.5.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	9.8	A path traversal vulnerability in ZKTeco BioTime v8.5.5 allows attackers to write arbitrary files via using a malicious SFTP configuration. **CVE ID : CVE-2023-38951**	N/A	A-ZKT-BIOT-220823/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	7.5	An issue in a hidden API in ZKTeco BioTime v8.5.5 allows unauthenticated attackers to arbitrarily reset the Administrator password via a crafted web request. **CVE ID : CVE-2023-38949**	N/A	A-ZKT-BIOT-220823/1780
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2023	7.5	A path traversal vulnerability in the iclock API of ZKTeco BioTime v8.5.5 allows unauthenticated attackers to read arbitrary files via supplying a crafted payload. **CVE ID : CVE-2023-38950**	N/A	A-ZKT-BIOT-220823/1781
Files or Directories Accessible to External Parties	03-Aug-2023	7.5	Insecure access control in ZKTeco BioTime v8.5.5 allows unauthenticated attackers to read sensitive backup files and access sensitive information such as user credentials via sending a crafted HTTP request to the static files resources of the system. **CVE ID : CVE-2023-38952**	N/A	A-ZKT-BIOT-220823/1782
Vendor: Zohocorp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: manageengine_adaudit_plus					
Affected Version(s): 7.1.1					
Incorrect Authorization	07-Aug-2023	7.5	The event analysis component in Zoho ManageEngine ADAudit Plus 7.1.1 allows an attacker to bypass audit detection by creating or renaming user accounts with a "$" symbol suffix. **CVE ID : CVE-2023-32783**	N/A	A-ZOH-MANA-220823/1783
Product: manageengine_admanager_plus					
Affected Version(s): * Up to (excluding) 7.2					
N/A	04-Aug-2023	6.5	Zoho ManageEngine ADManager Plus through 7201 allow authenticated users to take over another user's account via sensitive information disclosure. **CVE ID : CVE-2023-38332**	https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2023-38332.html	A-ZOH-MANA-220823/1784
Affected Version(s): 7.2					
N/A	04-Aug-2023	6.5	Zoho ManageEngine ADManager Plus through 7201 allow authenticated users to take over another user's account via sensitive information disclosure. **CVE ID : CVE-2023-38332**	https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2023-38332.html	A-ZOH-MANA-220823/1785
Product: manageengine_applications_manager					
Affected Version(s): * Up to (excluding) 16.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Zoho ManageEngine Applications Manager through 16530 allows reflected XSS while logged in. **CVE ID : CVE-2023-38333**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-38333.html	A-ZOH-MANA-220823/1786
Affected Version(s): 16.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2023	6.1	Zoho ManageEngine Applications Manager through 16530 allows reflected XSS while logged in. **CVE ID : CVE-2023-38333**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-38333.html	A-ZOH-MANA-220823/1787
Product: manageengine_network_configuration_manager					
Affected Version(s): 12.6					
Origin Validation Error	04-Aug-2023	8.8	An issue was discovered in Zoho ManageEngine Network Configuration Manager 12.6.165. The WebSocket endpoint allows Cross-site WebSocket hijacking. **CVE ID : CVE-2023-29505**	https://www.manageengine.com/itom/advisory/cve-2023-29505.html	A-ZOH-MANA-220823/1788
Vendor: Zoom					
Product: meeting_software_development_kit					
Affected Version(s): * Up to (excluding) 5.14.10					
N/A	08-Aug-2023	7.5	Improper input validation in Zoom	https://explore.zoom.us/en/	A-ZOO-MEET-220823/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SDK's before 5.14.10 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-39217**	trust/security/security-bulletin/	
Affected Version(s): * Up to (excluding) 5.14.7					
N/A	08-Aug-2023	7.5	Uncontrolled resource consumption in Zoom SDKs before 5.14.7 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-36533**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-MEET-220823/1790
Affected Version(s): * Up to (excluding) 5.15.0					
Cleartext Storage of Sensitive Information	08-Aug-2023	5.5	Cleartext storage of sensitive information in Zoom Client SDK for Windows before 5.15.0 may allow an authenticated user to enable an information disclosure via local access. **CVE ID : CVE-2023-39210**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-MEET-220823/1791
Affected Version(s): * Up to (excluding) 5.15.5					
Exposure of Resource to Wrong Sphere	08-Aug-2023	8.1	Exposure of sensitive information in Zoom Client SDK's before 5.15.5 may allow an authenticated user to enable a denial of	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-MEET-220823/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service via network access. **CVE ID : CVE-2023-39214**		
Product: rooms					
Affected Version(s): * Up to (excluding) 5.14.10					
N/A	08-Aug-2023	6.5	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow an authenticated user to enable information disclosure via network access. **CVE ID : CVE-2023-36535**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-220823/1793
N/A	08-Aug-2023	4.9	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow a privileged user to enable information disclosure via network access. **CVE ID : CVE-2023-39218**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-220823/1794
Affected Version(s): * Up to (excluding) 5.15.5					
Improper Privilege Management	08-Aug-2023	7.8	Improper privilege management in Zoom Desktop Client for Windows and Zoom Rooms for Windows before 5.15.5 may allow an	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-220823/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to enable an information disclosure via local access. **CVE ID : CVE-2023-39211**		
Untrusted Search Path	08-Aug-2023	5.5	Untrusted search path in Zoom Rooms for Windows before version 5.15.5 may allow an authenticated user to enable a denial of service via local access. **CVE ID : CVE-2023-39212**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-220823/1796
Affected Version(s): * Up to (excluding) 5.14.5					
Out-of-bounds Write	08-Aug-2023	7.5	Buffer overflow in Zoom Clients before 5.14.5 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-36532**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ROOM-220823/1797
Product: video_software_development_kit					
Affected Version(s): * Up to (excluding) 5.14.10					
N/A	08-Aug-2023	7.5	Improper input validation in Zoom SDK's before 5.14.10 may allow an unauthenticated user to enable a denial of	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIDE-220823/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service via network access. **CVE ID : CVE-2023-39217**		
Affected Version(s): * Up to (excluding) 5.14.7					
N/A	08-Aug-2023	7.5	Uncontrolled resource consumption in Zoom SDKs before 5.14.7 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-36533**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIDE-220823/1799
Product: virtual_desktop_infrastructure					
Affected Version(s): * Up to (excluding) 5.14.10					
N/A	08-Aug-2023	6.5	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow an authenticated user to enable information disclosure via network access. **CVE ID : CVE-2023-36535**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIRT-220823/1800
N/A	08-Aug-2023	4.9	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow a privileged user to enable information disclosure via network access.	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIRT-220823/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39218		
Affected Version(s): * Up to (excluding) 5.14.5					
Out-of-bounds Write	08-Aug-2023	7.5	Buffer overflow in Zoom Clients before 5.14.5 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-36532**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIRT-220823/1802
Affected Version(s): * Up to (excluding) 5.15.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Aug-2023	9.8	Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access. **CVE ID : CVE-2023-39213**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-VIRT-220823/1803
Product: zoom					
Affected Version(s): * Up to (excluding) 5.14.10					
N/A	08-Aug-2023	6.5	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow an authenticated user to	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable information disclosure via network access. **CVE ID : CVE-2023-36535**		
N/A	08-Aug-2023	4.9	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow a privileged user to enable information disclosure via network access. **CVE ID : CVE-2023-39218**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1805
Affected Version(s): * Up to (excluding) 5.14.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Aug-2023	9.8	Path traversal in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access. **CVE ID : CVE-2023-36534**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1806
N/A	08-Aug-2023	9.8	Improper input validation in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access. **CVE ID : CVE-2023-39216**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.15.5					
Improper Privilege Management	08-Aug-2023	7.8	Improper privilege management in Zoom Desktop Client for Windows and Zoom Rooms for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via local access. **CVE ID : CVE-2023-39211**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1808
Improper Input Validation	08-Aug-2023	6.5	Improper input validation in Zoom Desktop Client for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via network access. **CVE ID : CVE-2023-39209**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1809
Affected Version(s): * Up to (excluding) 5.14.5					
Insufficient Verification of Data Authenticity	08-Aug-2023	8.8	Insufficient verification of data authenticity in Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via network access.	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36541		
Untrusted Search Path	08-Aug-2023	7.8	Untrusted search path in the installer for Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access. **CVE ID : CVE-2023-36540**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1811
Out-of-bounds Write	08-Aug-2023	7.5	Buffer overflow in Zoom Clients before 5.14.5 may allow an unauthenticated user to enable a denial of service via network access. **CVE ID : CVE-2023-36532**	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1812
Affected Version(s): * Up to (excluding) 5.15.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Aug-2023	9.8	Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access.	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-220823/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39213		
Hardware					
Vendor: ABB					
Product: ac700f					
Affected Version(s): -					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects:	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	H-ABB-AC70-220823/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&Langu	H-ABB-AC70-220823/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 ,	ageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0426**		
Product: ac900f					
Affected Version(s): -					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	H-ABB-AC90-220823/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0425		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	H-ABB-AC90-220823/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0426**		
Vendor: Advantech					
Product: eki-1521					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**	N/A	H-ADV-EKI--220823/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface. **CVE ID : CVE-2023-4203**	N/A	H-ADV-EKI--220823/1819
Product: eki-1522					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**	N/A	H-ADV-EKI--220823/1820
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface.	N/A	H-ADV-EKI--220823/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4203		
Product: eki-1524					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**	N/A	H-ADV-EKI--220823/1822
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface. **CVE ID : CVE-2023-4203**	N/A	H-ADV-EKI--220823/1823
Vendor: AMD					
Product: *					
Affected Version(s): *					
Observable Discrepancy	01-Aug-2023	4.7	A potential power side-channel vulnerability in AMD processors may allow an authenticated	https://www.amd.com/en/corporate/product-security/bulle	H-AMD-*-220823/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to monitor the CPU power consumption as the data in a cache line changes over time potentially resulting in a leak of sensitive information. **CVE ID : CVE-2023-20583**	tin/AMD-SB-7006	
Vendor: assmann					
Product: ht-ip211hdp					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	04-Aug-2023	7.5	Assmann Digitus Plug&View IP Camera HT-IP211HDP, version 2.000.022 allows unauthenticated attackers to download a copy of the camera's settings and the administrator credentials. **CVE ID : CVE-2023-30146**	N/A	H-ASS-HT-I-220823/1825
Vendor: Asus					
Product: rt-ac66u_b1					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Aug-2023	7.5	ASUS RT-AC66U B1 3.0.0.4.286_51665 was discovered to transmit sensitive information in cleartext. **CVE ID : CVE-2023-39086**	N/A	H-ASU-RT-A-220823/1826
Vendor: Cisco					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: s195					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-S195-220823/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: s395					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-S395-220823/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: s695					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-S695-220823/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: spa500ds					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1830
Improper Neutralization of Input During Web Page Generation	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-	H-CIS-SPA5-220823/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]]	multi-7kvPmu2F	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20218		
Product: spa500s					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1832
Improper Neutralization of Input	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-SPA5-220823/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability.	/CiscoSecurity Advisory/cisco-sa-spa-web-multi-7kvPmu2F	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			{{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa501g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa502g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20181		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa504g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa508g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa509g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa512g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa514g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa525					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa525g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa525g2					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	H-CIS-SPA5-220823/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: web_security_appliance_s170					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s190					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s380					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s390					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s680					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s690					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: web_security_appliance_s690x					
Affected Version(s): -					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	H-CIS-WEB_-220823/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Vendor: connectedio					
Product: er2000t-vz-cat1					
Affected Version(s): -					
N/A	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has a misconfiguration in their MQTT broker used for management and device communication, which allows devices to connect to the broker and issue commands to other device, impersonating Connected IO management platform and sending commands to all of	N/A	H-CON-ER20-220823/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connected IO's devices. **CVE ID : CVE-2023-33379**		
Vendor: Emerson					
Product: dl8000					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	H-EME-DL80-220823/1862
Product: roc809					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	H-EME-ROC8-220823/1863
Product: roc809l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	H-EME-ROC8-220823/1864
Product: roc827					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	H-EME-ROC8-220823/1865
Product: roc827l					
Affected Version(s): -					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition.	N/A	H-EME-ROC8-220823/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1935		
Vendor: Epson					
Product: ep-801a					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-EP-8-220823/1867
Product: ep-802a					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer	https://www.epson.jp/support/misc_t/23	H-EPS-EP-8-220823/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	0802_oshirase.htm	
Product: ep-901a					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-EP-9-220823/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: ep-901f					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-EP-9-220823/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: ep-902a					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-EP-9-220823/1871
Product: pa-tcu1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PA-T-220823/1872
Product: pm-t960					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PM-T-220823/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: pm-t990					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PM-T-220823/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: px-201					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PX-2-220823/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: px-502a					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PX-5-220823/1876
Product: px-601f					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PX-6-220823/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: px-602f					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config	https://www.epson.jp/support/misc_t/230802_oshirase.htm	H-EPS-PX-6-220823/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Vendor: ezviz					
Product: cs-c6n-a0-1c2wfr-mul					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-c6n-b0-1g2wf					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-c6n-r101-1g2wf					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and	https://www.ezviz.com/data-security/security-	H-EZV-CS-C-220823/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware	notice/detail/827	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv248-a0-32wmfr					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg	https://www.ezviz.com/data-security/secur	H-EZV-CS-C-220823/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before	ity-notice/detail/827	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-1b2wfr					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-1c2wfr					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-1c2wfr-c					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34552		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-3c2wfrl-1080p					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-CS-C-220823/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34551		
Product: lc1c					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-LC1C-220823/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware	https://www.ezviz.com/data-security/security-notice/detail/827	H-EZV-LC1C-220823/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Vendor: F5					
Product: big-ip_10200v-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_10350v-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Product: big-ip_11000-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F,	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_11050-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_5250v-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_6900-f					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_7200v-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Product: big-ip_8900-f					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_i15820-df					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_i5820-df					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_i7820-df					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and	https://my.f5.com/manage/s/article/K000135449	H-F5-BIG--220823/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Vendor: gatesair					
Product: flexiva_fax_150w					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Aug-2023	9.8	An isssue in GatesAIr Flexiva FM Transmitter/Exiter Fax 150W allows a remote attacker to gain privileges via the LDAP and SMTP credentials. **CVE ID : CVE-2023-36082**	N/A	H-GAT-FLEX-220823/1908
Improper Neutralization of Input During	02-Aug-2023	5.4	Cross Site Scripting vulnerability in GatesAIr Flexiva FM Transmitter/Exciter v.FAX 150W allows a	N/A	H-GAT-FLEX-220823/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			remote attacker to execute arbitrary code via a crafted script to the web application dashboard. **CVE ID : CVE-2023-36081**		
Vendor: hpe					
Product: aruba_cx_10000-48y6					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1910
Product: aruba_cx_4100i					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1911
Product: aruba_cx_6000_12g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6000_24g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6000_48g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1914
Product: aruba_cx_6100					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1915
Product: aruba_cx_6200f					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6200f_48g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6200m					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1918
Product: aruba_cx_6200m_24g					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1919
Product: aruba_cx_6300m_24p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6300m_48g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_6405					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1922
Product: aruba_cx_6410					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1923
Product: aruba_cx_8320-32					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8320-48p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8325-32c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1926
Product: aruba_cx_8325-48y8c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1927
Product: aruba_cx_8360-12c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8360-16y2c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8360-24xf2c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1930
Product: aruba_cx_8360-32y4c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1931
Product: aruba_cx_8360-48xt4c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8360-48y6c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Product: aruba_cx_8400					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1934
Product: aruba_cx_9300_32d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	H-HPE-ARUB-220823/1935
Vendor: mediatek					
Product: mt2713					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1937
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**		
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1939
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1941
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1942
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**		
Product: mt2735					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1944
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Product: mt2737					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1946
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT27-220823/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20796		
Product: mt5221					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT52-220823/1948
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT52-220823/1949
Product: mt5583					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT55-220823/1950
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT55-220823/1951
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT55-220823/1952

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. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt5691					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1953
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1955
Product: mt5695					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1957
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT56-220823/1958
Product: mt6580					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1959
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1960
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT65-220823/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1962
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1964
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1966
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1967
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1969
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT65-220823/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**		
Product: mt6731					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1971
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1973
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1974
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	bulletin/August-2023	
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1976
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1978
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1980
Product: mt6737					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1982
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1983
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-220823/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1985
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1987
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1989
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1991
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1992
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1994
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1996
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1997
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.com	H-MED-MT67-220823/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/1999
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2001
Product: mt6753					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2003
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20780		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2005
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2006
Product: mt6757					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2007
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2008
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2010
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
Product: mt6757c					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2012
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2014
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2015
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	bulletin/August-2023	
Product: mt6757cd					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2017
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2019
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2021
Product: mt6757ch					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2023
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2024
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-220823/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2026
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2028
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2030
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2032
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2033
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2035
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2037
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2038
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.com	H-MED-MT67-220823/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2040
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2042
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**		
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2044
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2046
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2047
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT67-220823/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2049
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2051
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2053
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2055
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2056
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2058
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2060
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20814		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2062
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2063
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2065
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2067
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2069
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2070
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	bulletin/August-2023	
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2072
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**		
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2074
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2076
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2077
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2079
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2081
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2083
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2084
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2086
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2088
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2090
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2091
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2093
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2095
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20782		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2097
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2098
Product: mt6771					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2099
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2100
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2102
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2104
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2106
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2107
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2109
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2111
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20815		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2113
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2114
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2116
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2118
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2120
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2121
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	bulletin/August-2023	
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2123
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2125
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20786		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2127
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2128
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2130
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2132
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2134
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2135
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2137
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2139
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2141
Product: mt6783					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2142
Product: mt6785					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2143
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2144
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2146
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2148
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2149
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2151
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2153
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20812		
Product: mt6789					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2155
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2157
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2158
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of	https://corp.mediatek.com/product-security-	H-MED-MT67-220823/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2160
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2162
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT67-220823/2164
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2165
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2167
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2169
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20815		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2171
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2172
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2174
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2176
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2178
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2179
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2181
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**		
Product: mt6835					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2183
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2185
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2186
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2188
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2190
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2192
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2194
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2195
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2197
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2199
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2201
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2202
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2204
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2206
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2208
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2209
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2211
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**		
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2213
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2215
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2216
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2218
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2220
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20780		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2222
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2223
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2225
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2227
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2229
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2230
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2232
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2234
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20817		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2236
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2237
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2239
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2241
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20798		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2243
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2244
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	bulletin/August-2023	
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2246
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2248
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2250
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2252
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2253
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2255
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2257
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2258
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.com	H-MED-MT68-220823/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2260
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2262
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20812		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2264
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2265
Product: mt6875					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2266
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2267
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2269
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2271
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2273
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2274
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2276
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2278
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2280
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2281
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2283
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2285
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20814		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2287
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2288
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2290
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2292
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2294
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2295
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2297
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2299
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2301
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2302
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2304
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2306
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20804		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2308
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2309
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2311
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2313
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2315
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2316
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2318
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2320
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2321
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information	https://corp.mediatek.com	H-MED-MT68-220823/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2323
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2325
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20812		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2327
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2328
Product: mt6880					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2329
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2330
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2332
Out-of-bounds Write	07-Aug-2023	6.7	In gps, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2334
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2336
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2337
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2339
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2341
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2342
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.com	H-MED-MT68-220823/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2344
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2346
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2348
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2350
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2351
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2353
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2355
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20817		
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2357
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2358
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT68-220823/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2360
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2362
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20812		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2364
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2365
Product: mt6886					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2366
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2367
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2369
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2371
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2373
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2374
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2376
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2378
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2380
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2381
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2383
Product: mt6889					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2385
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2387
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2388
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2390
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2392
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2394
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2395
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2397
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2399
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2400
Product: mt6890					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2401
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2402
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2404
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2406
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20815		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2408
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2409
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2411
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2413
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2415
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2416
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	bulletin/August-2023	
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2418
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2420
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2422
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2424
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2425
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2427
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2429
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2431
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2432
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2434
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2436
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2438
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2439
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2441
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2443
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20806		
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2445
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2446
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-security-	H-MED-MT68-220823/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2448
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**		
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2450
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2452
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2453
Concurrent Execution using Shared Resource with Improper	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2455
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2457
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2459
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2460
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2462
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2464
Product: mt6896					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT68-220823/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20812		
Product: mt6980					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2466
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2467
Product: mt6983					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2468
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2469
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2471
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2473
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2475
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2476
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2478
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2480
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2481
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to	https://corp.mediatek.com/product-	H-MED-MT69-220823/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2483
Concurrent Execution using Shared Resource with Improper Synchronization	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2485
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20781		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2487
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2488
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT69-220823/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2490
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2492
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20813		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2494
Product: mt6985					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2496
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2497
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2499
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2501
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2503
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2504
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of	https://corp.mediatek.com/product-security-	H-MED-MT69-220823/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2506
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2508
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2510
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2511
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2513
Product: mt6990					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT69-220823/2515
Product: mt8167					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20786		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2517
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2518
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Product: mt8167s					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2520
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2522
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8168					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2524
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2525
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT81-220823/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2527
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2529
Product: mt8173					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2531
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2532
Product: mt8183					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2533
Product: mt8185					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2534
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT81-220823/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2536
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2538
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Product: mt8188					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2540
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2542
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2543
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**		
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2545
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**		
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2547
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2548
Concurrent Execution	07-Aug-2023	6.4	In imgsys, there is a possible use after	https://corp.mediatek.com	H-MED-MT81-220823/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	/product-security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2550
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2552
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20798		
Product: mt8195					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2554
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2556
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2557
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**		
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2559
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**		
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2561
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2562
Concurrent Execution	07-Aug-2023	6.4	In imgsys, there is a possible use after	https://corp.mediatek.com	H-MED-MT81-220823/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	/product-security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2564
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2566
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20798		
Product: mt8195z					
Affected Version(s): -					
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT81-220823/2568
Product: mt8321					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20783		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2570
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2571
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-220823/2572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2573
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2575
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2577
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2578
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-220823/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	bulletin/August-2023	
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2580
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2582
Product: mt8365					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20786		
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2584
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2585
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2587
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2589
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2591
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2593
Product: mt8395					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2594
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-220823/2595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2596
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**		
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2598
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2600
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2601
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT83-220823/2603
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2605
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20780		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2607
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2608
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT86-220823/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	bulletin/August-2023	
Product: mt8667					
Affected Version(s): -					
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2610
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2612
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2614
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20797		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2616
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2617
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT86-220823/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2619
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2621
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20781		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2623
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2624
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to	https://corp.mediatek.com/product-	H-MED-MT86-220823/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	security-bulletin/August-2023	
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2626
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2628
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2630
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT86-220823/2631
Product: mt8765					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2632
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2633
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-220823/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2635
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2637
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2639
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2641
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2642
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of	https://corp.mediatek.com/product-security-	H-MED-MT87-220823/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2644
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2646
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20784		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2648
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2649
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a	https://corp.mediatek.com/product-	H-MED-MT87-220823/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	security-bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2651
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2653
Product: mt8781					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2655
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2656
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system	https://corp.mediatek.com	H-MED-MT87-220823/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2658
Out-of-bounds Write	07-Aug-2023	6.4	In audio, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2660
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20780		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2662
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2663
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-220823/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2665
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2667
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2669
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2670
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.com	H-MED-MT87-220823/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	/product-security-bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2672
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2674
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2676
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2678
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2679
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**		
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2681
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2683
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20781		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2685
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2686
Product: mt8791					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2687
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2688
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2690
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2692
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2693
Product: mt8791t					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2694
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2695
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-220823/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2697
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2699
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20790		
Product: mt8797					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2701
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2703
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2704
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2706
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT87-220823/2708
Product: mt9010					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20809		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2710
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2711
Product: mt9011					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2712
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2713
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2715
Product: mt9012					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2717
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20810		
Product: mt9016					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2719
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2721
Product: mt9020					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2722
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT90-220823/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2724
Product: mt9021					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2726
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**		
Product: mt9022					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2728
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20809		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2730
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2731
Product: mt9030					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2732
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2733
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**		
Product: mt9031					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2735
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2737
Product: mt9032					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2739
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT90-220823/2740
Product: mt9215					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2741
Product: mt9216					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2743
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2744
Product: mt9218					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT92-220823/2745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2746
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**		
Product: mt9220					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2748
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2750
Product: mt9221					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20809		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2752
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2753
Product: mt9222					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2754
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2755
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**		
Product: mt9255					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2757
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2759
Product: mt9256					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2761
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2762
Product: mt9266					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2763
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2764
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT92-220823/2765

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. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9269					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2766
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2768
Product: mt9285					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Product: mt9286					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2770
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20811		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2772
Product: mt9288					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2774
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT92-220823/2775
Product: mt9600					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	bulletin/August-2023	
Product: mt9602					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2777
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2779
Product: mt9610					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2781
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9611					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2783
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2784
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9612					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2786
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2788
Product: mt9613					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2790
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9615					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2792
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2793
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9617					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2795
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2797
Product: mt9618					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2799
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9629					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2801
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2802
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9630					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2804
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2806
Product: mt9631					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2808
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9632					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2810
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2811
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9636					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2813
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2815
Product: mt9638					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2817
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9639					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2819
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2820
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9649					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2822
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2824
Product: mt9650					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2826
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9652					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2828
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2829
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9653					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2831
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2833
Product: mt9666					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2835
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt9667					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2837
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2838
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	bulletin/August-2023	
Product: mt9669					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2840
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2842
Product: mt9670					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**		
Product: mt9671					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2844
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20811		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2846
Product: mt9675					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2848
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2849
Product: mt9685					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT96-220823/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2851
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**		
Product: mt9686					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2853
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061;	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2855
Product: mt9688					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20809		
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2857
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	H-MED-MT96-220823/2858
Vendor: Mitsubishielectric					
Product: c80					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-C80-220823/2859
Product: e70					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-E70-220823/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3346		
Product: e80					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-E80-220823/2861
Product: gs21					
Affected Version(s): -					
Use of Insufficiently Random Values	04-Aug-2023	9.1	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT21 model versions 01.49.000 and prior and GOT SIMPLE Series GS21 model versions 01.49.000 and prior allows a remote unauthenticated attacker to hijack	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-006_en.pdf	H-MIT-GS21-220823/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it. **CVE ID : CVE-2023-3373**		
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GS21-220823/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gs25					
Affected Version(s): -					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GS25-220823/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Insufficiently Random Values	04-Aug-2023	9.1	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT21 model versions 01.49.000 and prior and GOT SIMPLE Series GS21 model versions 01.49.000 and prior allows a remote unauthenticated attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it. **CVE ID : CVE-2023-3373**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-006_en.pdf	H-MIT-GT21-220823/2865
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GT21-220823/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gt23					
Affected Version(s): -					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GT23-220823/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt25					
Affected Version(s): -					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GT25-220823/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt27					
Affected Version(s): -					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	H-MIT-GT27-220823/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0525		
Product: m70v					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M70V-220823/2870
Product: m720vs					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M720-220823/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m720vs_15-type					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M720-220823/2872
Product: m720vw					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M720-220823/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m730vs					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M730-220823/2874
Product: m730vs_15-type					
Affected Version(s): -					
Buffer Copy without Checking Size of	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-M730-220823/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	lity/pdf/2023-007_en.pdf	
Product: m730vw					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M730-220823/2876
Product: m750vs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M750-220823/2877
Product: m750vs_15-type					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M750-220823/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3346		
Product: m750vw					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M750-220823/2879
Product: m80					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M80-220823/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m800s					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M800-220823/2881
Product: m800vs					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M800-220823/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m800vw					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M800-220823/2883
Product: m800w					
Affected Version(s): -					
Buffer Copy without Checking Size of	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in	https://www.mitsubishielectric.com/en/psirt/vulnerabi	H-MIT-M800-220823/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	lity/pdf/2023-007_en.pdf	
Product: m80v					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M80V-220823/2885
Product: m80vw					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M80V-220823/2886
Product: m80w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery.	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	H-MIT-M80W-220823/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3346		
Vendor: Netgear					
Product: dc112a					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi. **CVE ID : CVE-2023-38925**	https://www.netgear.com/about/security/	H-NET-DC11-220823/2888
Product: dg834gv5					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DG834Gv5 1.6.01.34 was discovered to contain multiple buffer overflows via the wla_ssid and wla_temp_ssid parameters at bsw_ssid.cgi. **CVE ID : CVE-2023-38591**	https://www.netgear.com/about/security/	H-NET-DG83-220823/2889
Product: dgn3500					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	07-Aug-2023	6.5	Netgear DGN3500 1.1.00.37 was discovered to contain a buffer overflow via the http_password	https://www.netgear.com/about/security/	H-NET-DGN3-220823/2890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			parameter at setup.cgi. **CVE ID : CVE-2023-38924**		
Product: ex6200					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi. **CVE ID : CVE-2023-38925**	https://www.netgear.com/about/security/	H-NET-EX62-220823/2891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set. **CVE ID : CVE-2023-38926**	https://www.netgear.com/about/security/	H-NET-EX62-220823/2892
Product: jwnr2000v2					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and	https://www.netgear.com/about/security/	H-NET-JWNR-220823/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function. **CVE ID : CVE-2023-39550**	https://www.netgear.com/about/security/	H-NET-JWNR-220823/2894
Product: r6300v2					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi. **CVE ID : CVE-2023-38925**	https://www.netgear.com/about/security/	H-NET-R630-220823/2895
Product: r6900p					
Affected Version(s): -					
Buffer Copy without Checking	07-Aug-2023	8.8	Netgear R6900P v1.3.3.154 was discovered to contain multiple	https://www.netgear.com/a	H-NET-R690-220823/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			buffer overflows via the wla_ssid and wlg_ssid parameters at ia_ap_setting.cgi. **CVE ID : CVE-2023-38412**	bout/security/	
Product: r7100lg					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Aug-2023	9.8	Netgear R7100LG 1.0.0.78 was discovered to contain a command injection vulnerability via the password parameter at usb_remote_invite.cgi. **CVE ID : CVE-2023-38928**	https://www.netgear.com/about/security/	H-NET-R710-220823/2897
Product: wag302v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Aug-2023	8.8	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler function via the firmwareRestore and firmwareServerip parameters. **CVE ID : CVE-2023-38921**	https://www.netgear.com/about/security/	H-NET-WAG3-220823/2898
Product: wg302v2					
Affected Version(s): -					
Improper Neutralizat	07-Aug-2023	8.8	Netgear WG302v2 v5.2.9 and	https://www.netgear.com/a	H-NET-WG30-220823/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler function via the firmwareRestore and firmwareServerip parameters. **CVE ID : CVE-2023-38921**	bout/security/	
Product: xavn2001v2					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**	https://www.netgear.com/about/security/	H-NET-XAVN-220823/2900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username	https://www.netgear.com/about/security/	H-NET-XAVN-220823/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters in the check_auth function. **CVE ID : CVE-2023-39550**		
Product: xr300					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear XR300 v1.0.3.78 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at genie_ap_wifi_change.cgi. **CVE ID : CVE-2023-36499**	https://www.netgear.com/about/security/	H-NET-XR30-220823/2902
Product: xwn5001					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**	https://www.netgear.com/about/security/	H-NET-XWN5-220823/2903
Buffer Copy without Checking Size of	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2	https://www.netgear.com/about/security/	H-NET-XWN5-220823/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function. **CVE ID : CVE-2023-39550**		
Vendor: Omron					
Product: cj1w-eip21					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ1W-220823/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu64-eip					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2H-220823/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu65-eip					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2H-220823/2907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu66-eip					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2H-220823/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu67-eip					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of	https://www.ia.omron.com/product/vulnerability/OMSR	H-OMR-CJ2H-220823/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**	-2023-006_en.pdf	
Product: cj2h-cpu68-eip					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2H-220823/2910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu31					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2M-220823/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu32					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2M-220823/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu33					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2M-220823/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu34					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2M-220823/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu35					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CJ2M-220823/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cs1w-eip21					
Affected Version(s): -					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	H-OMR-CS1W-220823/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Vendor: oppo					
Product: find_x3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	9.8	There is a command injection problem in the old version of the mobile phone backup app. **CVE ID : CVE-2023-26310**	https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1684402464721477632	H-OPP-FIND-220823/2917
Vendor: Phoenixcontact					
Product: cloud_client_1101t-tx					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-CLOU-220823/2918
Improper Restriction of Recursive Entity References in DTDs ('XML	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior	N/A	H-PHO-CLOU-220823/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Expansion')			to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_C-220823/2920
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated	N/A	H-PHO-TC_C-220823/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Expansion')			remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g_att					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_C-220823/2922
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges	N/A	H-PHO-TC_C-220823/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g_vzw					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_C-220823/2924
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file	N/A	H-PHO-TC_C-220823/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_router_3002t-4g					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_R-220823/2926
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service.	N/A	H-PHO-TC_R-220823/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3569		
Product: tc_router_3002t-4g_att					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_R-220823/2928
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**	N/A	H-PHO-TC_R-220823/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tc_router_3002t-4g_vzw					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	H-PHO-TC_R-220823/2930
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**	N/A	H-PHO-TC_R-220823/2931
Product: wp_6070-wvps					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	H-PHO-WP_6-220823/2932
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	H-PHO-WP_6-220823/2933
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device.	N/A	H-PHO-WP_6-220823/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3571		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	H-PHO-WP_6-220823/2935
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	H-PHO-WP_6-220823/2936
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-	N/A	H-PHO-WP_6-220823/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/2938
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s).	N/A	H-PHO-WP_6-220823/2939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37857		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	H-PHO-WP_6-220823/2940
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	H-PHO-WP_6-220823/2941
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP	N/A	H-PHO-WP_6-220823/2942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to gain full access to the device. **CVE ID : CVE-2023-37864**		
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	H-PHO-WP_6-220823/2943
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	H-PHO-WP_6-220823/2944
Externally Controlled Reference	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in	N/A	H-PHO-WP_6-220823/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Resource in Another Sphere			versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**		
Product: wp_6101-wxps					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	H-PHO-WP_6-220823/2946
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to	N/A	H-PHO-WP_6-220823/2947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			gain full access to the device. **CVE ID : CVE-2023-3570**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	H-PHO-WP_6-220823/2948
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	H-PHO-WP_6-220823/2949
Improper Neutralization of Special Elements used in an OS Command	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with	N/A	H-PHO-WP_6-220823/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**		
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	H-PHO-WP_6-220823/2951
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/2952
Use of Hard-	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in	N/A	H-PHO-WP_6-220823/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	H-PHO-WP_6-220823/2954
Improper Neutralization of Special Elements used in an OS	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write	N/A	H-PHO-WP_6-220823/2955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**		
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	H-PHO-WP_6-220823/2956
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	H-PHO-WP_6-220823/2957
Externally Controlled Reference	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in	N/A	H-PHO-WP_6-220823/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Resource in Another Sphere			versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	H-PHO-WP_6-220823/2959
Product: wp_6121-wxps					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to	N/A	H-PHO-WP_6-220823/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	H-PHO-WP_6-220823/2961
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	H-PHO-WP_6-220823/2962
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to	N/A	H-PHO-WP_6-220823/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	H-PHO-WP_6-220823/2964
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	H-PHO-WP_6-220823/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/2966
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	H-PHO-WP_6-220823/2967
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges	N/A	H-PHO-WP_6-220823/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	H-PHO-WP_6-220823/2969
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	H-PHO-WP_6-220823/2970
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with	N/A	H-PHO-WP_6-220823/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	H-PHO-WP_6-220823/2972
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser .	N/A	H-PHO-WP_6-220823/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37856		
Product: wp_6156-whps					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	H-PHO-WP_6-220823/2974
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	H-PHO-WP_6-220823/2975
Improper Neutralization of Special Elements used in an OS Command	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST	N/A	H-PHO-WP_6-220823/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	H-PHO-WP_6-220823/2977
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	H-PHO-WP_6-220823/2978
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to	N/A	H-PHO-WP_6-220823/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/2980
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be	N/A	H-PHO-WP_6-220823/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	H-PHO-WP_6-220823/2982
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	H-PHO-WP_6-220823/2983
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with	N/A	H-PHO-WP_6-220823/2984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**		
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	H-PHO-WP_6-220823/2985
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	H-PHO-WP_6-220823/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	H-PHO-WP_6-220823/2987
Product: wp_6185-whps					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	H-PHO-WP_6-220823/2988
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a	N/A	H-PHO-WP_6-220823/2989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	H-PHO-WP_6-220823/2990
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	H-PHO-WP_6-220823/2991
Improper Neutralization of Special Elements used in an	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated	N/A	H-PHO-WP_6-220823/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**		
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	H-PHO-WP_6-220823/2993
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	H-PHO-WP_6-220823/2995
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	H-PHO-WP_6-220823/2996
Improper Neutralization of Special	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to	N/A	H-PHO-WP_6-220823/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**		
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	H-PHO-WP_6-220823/2998
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	H-PHO-WP_6-220823/2999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	H-PHO-WP_6-220823/3000
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	H-PHO-WP_6-220823/3001
Product: wp_6215-whps					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use	N/A	H-PHO-WP_6-220823/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	H-PHO-WP_6-220823/3003
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	H-PHO-WP_6-220823/3004
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a	N/A	H-PHO-WP_6-220823/3005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	H-PHO-WP_6-220823/3006
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service.	N/A	H-PHO-WP_6-220823/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37862		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	H-PHO-WP_6-220823/3008
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	H-PHO-WP_6-220823/3009
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP	N/A	H-PHO-WP_6-220823/3010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	H-PHO-WP_6-220823/3011
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	H-PHO-WP_6-220823/3012
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an	N/A	H-PHO-WP_6-220823/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	H-PHO-WP_6-220823/3014
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog	N/A	H-PHO-WP_6-220823/3015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the embedded Qt browser . **CVE ID : CVE-2023-37856**		
Vendor: Qualcomm					
Product: 205					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-205-220823/3016
Product: 215					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-215-220823/3017
Product: 315_5g_iot_modem					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-315_-220823/3018
Product: 8098					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-8098-220823/3019
Product: 8998					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-8998-220823/3020
Product: apq5053-aa					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ5-220823/3021
Product: apq8009					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3022
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3023
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3024
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3025
Product: apq8017					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-APQ8-220823/3026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3027
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3028
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3029
Product: apq8037					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3031
Product: apq8053-aa					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3032
Product: apq8053-ac					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3033
Product: apq8064au					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3034
Product: apq8096au					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3035
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3036
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-APQ8-220823/3037
Product: aqt1000					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3038
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3039
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/	H-QUA-AQT1-220823/3040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3041
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3042
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3043
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3044
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3046
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AQT1-220823/3047
Product: ar8031					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3048
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3050
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3051
Product: ar8035					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3052
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3053
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3055
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3056
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-AR80-220823/3057
Product: c-v2x_9150					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-C-V2-220823/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: csra6620					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3059
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3060
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3061
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3062
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3064
Product: csra6640					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3065
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3066
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3067
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	H-QUA-CSRA-220823/3068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3069
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRA-220823/3070
Product: csrb31024					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRB-220823/3071
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRB-220823/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRB-220823/3073
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-CSRB-220823/3074
Product: fastconnect_6200					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3075
Product: fastconnect_6800					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3077
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read/write issues. **CVE ID : CVE-2023-28576**		
Product: fastconnect_6900					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3079
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3080
Time-of-check Time-of-	08-Aug-2023	7	The buffer obtained from kernel APIs such as	https://www.qualcomm.com/company/	H-QUA-FAST-220823/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	product-security/bulletins/august-2023-bulletin	
Product: fastconnect_7800					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3082
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FAST-220823/3084
Product: flight_rb5_5g_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FLIG-220823/3085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537		
Product: fsm10056					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-FSM1-220823/3086
Product: mdm8207					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM8-220823/3087
Product: mdm9205					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3088
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	H-QUA-MDM9-220823/3089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3090
Product: mdm9206					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3091
Product: mdm9207					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3092
Product: mdm9250					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3093
Product: mdm9607					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3094
Product: mdm9628					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3095
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3096
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	H-QUA-MDM9-220823/3097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3098
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3099
Product: mdm9650					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3100
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MDM9-220823/3101
Product: msm8108					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3102
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3103
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3104
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3105
Product: msm8208					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-MSM8-220823/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3107
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3108
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3109
Product: msm8209					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3110
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-220823/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3112
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3113
Product: msm8608					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3114
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3116
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3117
Product: msm8917					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3118
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3119
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	H-QUA-MSM8-220823/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3121
Product: msm8920					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3122
Product: msm8937					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3123
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-MSM8-220823/3124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: msm8940					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3125
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3126
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3127
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-MSM8-220823/3128
Product: pm8937					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-PM89-220823/3129
Product: qam8295p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3130
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3131
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3132
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QAM8-220823/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3134
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3135
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3136
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QAM8-220823/3137
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-QAM8-220823/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: qca4004					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3139
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3140
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3141
Product: qca4010					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-	https://www.qualcomm.com/company/product-	H-QUA-QCA4-220823/3142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while the device receives DNS response. **CVE ID : CVE-2023-21625**	security/bulletins/august-2023-bulletin	
Product: qca4020					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3143
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3144
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3145
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3146
Product: qca4024					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3147
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA4-220823/3148
Product: qca6174a					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3149
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3150
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3152
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3153
Product: qca6310					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3154
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3155
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	H-QUA-QCA6-220823/3156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3157
Product: qca6320					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3158
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3159
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3160
Product: qca6335					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3161
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3162
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3163
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3164
Product: qca6390					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3166
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3167
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3168
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3169
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3171
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3172
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3173
Product: qca6391					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3174
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21648	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3176
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3177
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3178
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3179
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3180
Access of Resource	08-Aug-2023	7.8	The cam_get_device_priv	https://www.qualcomm.co	H-QUA-QCA6-220823/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	m/company/product-security/bulletins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3182
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3183
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-QCA6-220823/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3185
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3186
Product: qca6420					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	H-QUA-QCA6-220823/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3188
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3189
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3190
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3191
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666		
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3193
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3194
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3195
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3196
Product: qca6421					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3197
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3198
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3199
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3200
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3202
Product: qca6426					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3203
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3204
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3205
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3207
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3208
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3209
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3211
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3212
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28576		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3214
Product: qca6430					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3215
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3216
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3217
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21650	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3219
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3220
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3221
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3222
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while	https://www.qualcomm.com/company/product-	H-QUA-QCA6-220823/3223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3224
Product: qca6431					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3225
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3226
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3228
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3229
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3230
Product: qca6436					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3231
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3233
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3234
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3235
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3236
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3238
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3239
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3241
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3242
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3243
Product: qca6564					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3244
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3245
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3246
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3247
Product: qca6564a					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3249
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3250
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3251
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3252
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3254
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3255
Product: qca6564au					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3256
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3257
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3259
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3260
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3261
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3262
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3264
Product: qca6574					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3265
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3266
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3267
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3269
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3270
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3271
Product: qca6574a					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3272
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3274
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3275
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3276
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3277
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3279
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3280
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3281
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3282
Product: qca6574au					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling service API with invalid address. **CVE ID : CVE-2023-21627**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3284
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3285
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3286
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3287
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3289
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3290
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3291
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3292
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3294
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3295
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3296
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3298
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3299
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3300
Product: qca6595					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3301
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3302
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type	https://www.qualcomm.com/company/	H-QUA-QCA6-220823/3303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3304
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3305
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3306
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3307
Product: qca6595au					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3308
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3309
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3310
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3311
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3312
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3314
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3315
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3316
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3317
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3319
Product: qca6696					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3320
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3321
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3322
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA6-220823/3323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3324
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3325
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3326
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3327
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3329
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3330
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3331
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3332
Product: qca6698aq					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3333
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA6-220823/3334
Product: qca8081					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3335
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3336
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3338
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3339
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3340
Product: qca8337					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3341
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA8-220823/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3343
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3344
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3345
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3346
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA8-220823/3347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA8-220823/3348
Product: qca9367					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3349
Product: qca9377					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3350
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCA9-220823/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3352
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3353
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3354
Product: qca9379					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3355
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	H-QUA-QCA9-220823/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3357
Product: qca9984					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCA9-220823/3358
Product: qcc5100					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3359
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3361
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3362
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3363
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3364
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCC5-220823/3365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcm2290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM2-220823/3366
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM2-220823/3367
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM2-220823/3368
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM2-220823/3369
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM2-220823/3370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Product: qcm4290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3371
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3372
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3373
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3374
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCM4-220823/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: qcm4325					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3376
Product: qcm4490					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM4-220823/3377
Product: qcm6125					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3378
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3380
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3381
Product: qcm6490					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3382
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3383
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCM6-220823/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3385
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCM6-220823/3386
Product: qcn6024					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN6-220823/3387
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN6-220823/3388
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-QCN6-220823/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: qcn7606					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	9.8	Memory corruption in QESL while processing payload from external ESL device to firmware. **CVE ID : CVE-2023-28561**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN7-220823/3390
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN7-220823/3391
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN7-220823/3392
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN7-220823/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Product: qcn9011					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3394
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3395
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3396
Product: qcn9012					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3397
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	H-QUA-QCN9-220823/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3399
Product: qcn9024					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3400
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3401
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3402
Product: qcn9074					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3403
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3404
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3405
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3406
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3408
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCN9-220823/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: qcs2290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS2-220823/3410
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS2-220823/3411
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS2-220823/3412
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS2-220823/3413
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCS2-220823/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: qcs405					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3415
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3416
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3417
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3419
Product: qcs410					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3420
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3421
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3422
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3424
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3425
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3427
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3428
Product: qcs4290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3430
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3431
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3432
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS4-220823/3433
Product: qcs4490					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QCS4-220823/3434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Product: qcs603					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3435
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3436
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3437
Product: qcs605					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3439
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3440
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3441
Product: qcs610					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3442
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3444
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3445
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3446
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3448
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3449
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: qcs6125					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3451
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3452
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3453
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3454
Product: qcs6490					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3455
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3456
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3457
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3458
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS6-220823/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8155					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS8-220823/3460
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS8-220823/3461
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCS8-220823/3462
Product: qcx315					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCX3-220823/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCX3-220823/3464
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QCX3-220823/3465
Product: qm215					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QM21-220823/3466
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QM21-220823/3467
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-QM21-220823/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: qrb5165					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3469
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3470
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3471
Product: qrb5165m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3473
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3474
Product: qrb5165n					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3475
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3476
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QRB5-220823/3477
Product: qsm8250					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3478
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3479
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3480
Product: qsm8350					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3481
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QSM8-220823/3483
Product: qts110					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-QTS1-220823/3484
Product: s820a					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-S820-220823/3485
Product: sa4150p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA41-220823/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3487
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3488
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3489
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3490
Product: sa4155p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	H-QUA-SA41-220823/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3492
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3493
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3494
Product: sa415m					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3495
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	H-QUA-SA41-220823/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA41-220823/3497
Product: sa515m					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA51-220823/3498
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA51-220823/3499
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA51-220823/3500
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	H-QUA-SA51-220823/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Product: sa6145p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3502
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3503
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3504
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3505
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	H-QUA-SA61-220823/3506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3507
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3508
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3509
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3511
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3512
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3513
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3514
Product: sa6150p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA61-220823/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling service API with invalid address. **CVE ID : CVE-2023-21627**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3516
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3517
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3518
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3519
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3521
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3522
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3523
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3524
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA61-220823/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3526
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3527
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3528
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3529
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	H-QUA-SA61-220823/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3531
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3532
Product: sa6155p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3533
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3535
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3536
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3537
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3538
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3539
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA61-220823/3540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3541
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3542
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3543
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA61-220823/3545
Product: sa8145p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3546
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3547
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3548
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3550
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3551
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3552
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3553
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3555
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3556
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3557
Product: sa8150p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3558
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA81-220823/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in automotive during system call. **CVE ID : CVE-2023-21643**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3560
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3561
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3562
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3563
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3565
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3566
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3567
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3568
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA81-220823/3569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3570
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3571
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3572
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3573
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	H-QUA-SA81-220823/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3575
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3576
Product: sa8155p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3577
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3579
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3580
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3581
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3582
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3583
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA81-220823/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3585
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3586
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3587
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3589
Product: sa8195p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3590
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3591
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3592
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3594
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3595
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3596
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3597
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3599
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3600
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA81-220823/3601
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3602
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA82-220823/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3604
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3605
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3606
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3608
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3609
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA82-220823/3610
Product: sa8540p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA85-220823/3611
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SA85-220823/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA85-220823/3613
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA85-220823/3614
Product: sa9000p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA90-220823/3615
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA90-220823/3616
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	H-QUA-SA90-220823/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SA90-220823/3618
Product: sc8180x\+sdx55					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SC81-220823/3619
Product: sd205					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD20-220823/3620
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD20-220823/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD20-220823/3622
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD20-220823/3623
Product: sd210					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD21-220823/3624
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD21-220823/3625
Access of Resource Using Incompatib	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of	https://www.qualcomm.com/company/product-	H-QUA-SD21-220823/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD21-220823/3627
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD21-220823/3628
Product: sd212					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD21-220823/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Product: sd429					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD42-220823/3630
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD42-220823/3631
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD42-220823/3632
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD42-220823/3633
Product: sd439					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD43-220823/3634
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD43-220823/3635
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD43-220823/3636
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD43-220823/3637
Product: sd450					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD45-220823/3638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD45-220823/3639
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD45-220823/3640
Product: sd460					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD46-220823/3641
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD46-220823/3642
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD46-220823/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD46-220823/3644
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD46-220823/3645
Product: sd480					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD48-220823/3646
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD48-220823/3647
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	H-QUA-SD48-220823/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD48-220823/3649
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD48-220823/3650
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD48-220823/3651
Product: sd625					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3653
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3654
Product: sd626					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3655
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3656
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD62-220823/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Product: sd632					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD63-220823/3658
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD63-220823/3659
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD63-220823/3660
Product: sd660					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3661
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	H-QUA-SD66-220823/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3663
Product: sd662					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3664
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3665
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3666
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	H-QUA-SD66-220823/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3668
Product: sd665					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3669
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3670
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3672
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD66-220823/3673
Product: sd670					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3674
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3675
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD67-220823/3676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3677
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3678
Product: sd675					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3679
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3680
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	H-QUA-SD67-220823/3681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3682
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3683
Product: sd678					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3684
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3686
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3687
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD67-220823/3688
Product: sd680					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD68-220823/3689
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD68-220823/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD68-220823/3691
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD68-220823/3692
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD68-220823/3693
Product: sd690_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3694
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	H-QUA-SD69-220823/3695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3696
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3697
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3698
Product: sd695					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3699
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to	https://www.qualcomm.co	H-QUA-SD69-220823/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3701
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3702
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3703
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD69-220823/3704
Product: sd710					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD71-220823/3705
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD71-220823/3706
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD71-220823/3707
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD71-220823/3708
Product: sd720g					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD72-220823/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD72-220823/3710
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD72-220823/3711
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD72-220823/3712
Product: sd730					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD73-220823/3713
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	H-QUA-SD73-220823/3714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD73-220823/3715
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD73-220823/3716
Product: sd750g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD75-220823/3717
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD75-220823/3718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD75-220823/3719
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD75-220823/3720
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD75-220823/3721
Product: sd765					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3722
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD76-220823/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3724
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3725
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3726
Product: sd765g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3727
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	H-QUA-SD76-220823/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3729
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3730
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3731
Product: sd768g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3733
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3734
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3735
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD76-220823/3736
Product: sd778g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD77-220823/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD77-220823/3738
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD77-220823/3739
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD77-220823/3740
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD77-220823/3741
Product: sd780g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	H-QUA-SD78-220823/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD78-220823/3743
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD78-220823/3744
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD78-220823/3745
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD78-220823/3746
Product: sd7c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD7C-220823/3747
Product: sd835					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD83-220823/3748
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD83-220823/3749
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD83-220823/3750
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD83-220823/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: sd845					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD84-220823/3752
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD84-220823/3753
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD84-220823/3754
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD84-220823/3755
Product: sd850					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3756
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3757
Product: sd855					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3758
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3759
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3761
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3762
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3763
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3764
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3766
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD85-220823/3767
Product: sd865_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3768
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3769
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	H-QUA-SD86-220823/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3771
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3772
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3773
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3775
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3776
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3777
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3779
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD86-220823/3780
Product: sd870					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SD87-220823/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3782
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3783
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3784
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3785
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3787
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3788
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD87-220823/3789
Product: sd888					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3790
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	H-QUA-SD88-220823/3791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3792
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3793
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3794
Product: sd888_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3795
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to	https://www.qualcomm.co	H-QUA-SD88-220823/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3797
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3798
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD88-220823/3799
Product: sda429w					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3801
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3802
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3803
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3804
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA4-220823/3805
Product: sda845					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDA8-220823/3806
Product: sdm429w					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM4-220823/3807
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM4-220823/3808
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM4-220823/3809
Product: sdm630					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SDM6-220823/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM6-220823/3811
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM6-220823/3812
Product: sdm845					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDM8-220823/3813
Product: sdx12					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX1-220823/3814
Product: sdx24					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX2-220823/3815
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX2-220823/3816
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX2-220823/3817
Product: sdx50m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3818
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SDX5-220823/3819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3820
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3821
Product: sdx55					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3822
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3823
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SDX5-220823/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3825
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3826
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3827
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3829
Product: sdx55m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3830
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3831
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3832
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3834
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3835
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3836
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX5-220823/3837
Product: sdx57m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SDX5-220823/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Product: sdx65					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX6-220823/3839
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX6-220823/3840
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX6-220823/3841
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDX6-220823/3842
Product: sdxr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3843
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3844
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3845
Product: sdxr2_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3846
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SDXR-220823/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3848
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3849
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3850
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3851
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SDXR-220823/3853
Product: sd_455					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_4-220823/3854
Product: sd_636					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3855
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3857
Product: sd_675					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3858
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3859
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3860
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_6-220823/3862
Product: sd_8cx					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3863
Product: sd_8cx_gen2					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3864
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd_8cx_gen3					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3866
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3867
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3868
Product: sd_8_gen1_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3869
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type	https://www.qualcomm.com/company/	H-QUA-SD_8-220823/3870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3871
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3872
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3873
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SD_8-220823/3874
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is	https://www.qualcomm.com/company/product-	H-QUA-SD_8-220823/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received due to improper input validation. **CVE ID : CVE-2023-21647**	security/bulletins/august-2023-bulletin	
Product: sg4150p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SG41-220823/3876
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SG41-220823/3877
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SG41-220823/3878
Product: sm4125					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM41-220823/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM41-220823/3880
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM41-220823/3881
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM41-220823/3882
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM41-220823/3883
Product: sm4350					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	H-QUA-SM43-220823/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm4350-ac					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3885
Product: sm4375					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3886
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3887
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3889
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3890
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM43-220823/3891
Product: sm4450					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM44-220823/3892
Product: sm6225					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	H-QUA-SM62-220823/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm6225-ad					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3894
Product: sm6250					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3895
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3896
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3898
Product: sm6250p					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3899
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3900
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM62-220823/3901
Product: sm6375					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	H-QUA-SM63-220823/3902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm7250p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM72-220823/3903
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM72-220823/3904
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM72-220823/3905
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM72-220823/3906
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-SM72-220823/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: sm7315					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3908
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3909
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3910
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3912
Product: sm7325p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3913
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3914
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3915
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM73-220823/3917
Product: sm8350					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM83-220823/3918
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM83-220823/3919
Product: sm8350-ac					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM83-220823/3920
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	H-QUA-SM83-220823/3921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm8450					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM84-220823/3922
Product: sm8475					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SM84-220823/3923
Product: smart_audio_100_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SMAR-220823/3924
Product: snapdragon_855					
Affected Version(s): -					
Access of Resource Using Incompatible Type	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-220823/3925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	tins/august-2023-bulletin	
Product: snapdragon_855\+\/860					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3926
Product: snapdragon_865\+_5g					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3927
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_REL	https://www.qualcomm.com/company/	H-QUA-SNAP-220823/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3929
Product: snapdragon_865_5g					
Affected Version(s): -					
Access of Resource	08-Aug-2023	7.8	The cam_get_device_priv	https://www.qualcomm.co	H-QUA-SNAP-220823/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	m/company/product-security/bulletins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3931
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count),	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Product: snapdragon_870_5g					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3933
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28577		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3935
Product: snapdragon_8_gen_1					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3936
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_REL	https://www.qualcomm.com/company/	H-QUA-SNAP-220823/3937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3938
Product: snapdragon_ar2_gen_1_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3939
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3940
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3941
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3942
Product: snapdragon_w5\+_gen_1					
Affected Version(s): -					
Access of Resource Using Incompatible Type	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-220823/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	tins/august-2023-bulletin	
Product: snapdragon_w5\+_gen_1_wearable_platform					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3944
Product: snapdragon_wear_4100\+					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3945
Product: snapdragon_wear_4100\+_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SNAP-220823/3946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3947
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3948
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3949
Product: snapdragon_x55_5g					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3951
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read/write issues. **CVE ID : CVE-2023-28576**		
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3953
Product: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3954
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3955
Product: snapdragon_xr1_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3957
Product: snapdragon_xr2_5g					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3958
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28577		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3960
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3961
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SNAP-220823/3962
Product: ssg2115p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SSG2-220823/3963
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SSG2-220823/3964
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SSG2-220823/3965
Product: ssg2125p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SSG2-220823/3966
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SSG2-220823/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SSG2-220823/3968
Product: sw5100					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3969
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3970
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3971
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SW51-220823/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21650	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3973
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3974
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3976
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3977
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3978
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is	https://www.qualcomm.com/company/product-	H-QUA-SW51-220823/3979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received due to improper input validation. **CVE ID : CVE-2023-21647**	security/bulletins/august-2023-bulletin	
Product: sw5100p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3980
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3981
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3982
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3983
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SW51-220823/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3985
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3986
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SW51-220823/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3988
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3989
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SW51-220823/3990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sxr1120					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR1-220823/3991
Product: sxr1230p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR1-220823/3992
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR1-220823/3993
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR1-220823/3994
Product: sxr2130					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/3995
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/3996
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/3997
Time-of-check Time-of-	08-Aug-2023	7	The buffer obtained from kernel APIs such as	https://www.qualcomm.com/company/	H-QUA-SXR2-220823/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	product-security/bulletins/august-2023-bulletin	
Product: sxr2150p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/3999
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/4000
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-SXR2-220823/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/4002
Product: sxr2230p					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-SXR2-220823/4003
Product: wcd9306					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4004
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21625		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4006
Product: wcd9326					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4007
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4008
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4009
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4011
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4012
Product: wcd9330					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4013
Product: wcd9335					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4015
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4016
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4017
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4018
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: wcd9340					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4020
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4021
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4022
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4023
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	H-QUA-WCD9-220823/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Product: wcd9341					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4025
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4026
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4027
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4028
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	H-QUA-WCD9-220823/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4030
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4031
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4032
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4034
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4035
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4037
Product: wcd9360					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4038
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4039
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4041
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4042
Product: wcd9370					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4043
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4044
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4046
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4047
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4048
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4050
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4051
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4052
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4054
Product: wcd9371					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4055
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4056
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: wcd9375					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4058
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4059
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4060
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4061
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4063
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4064
Product: wcd9380					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4065
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4066
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	H-QUA-WCD9-220823/4067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4068
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4069
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4070
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4072
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4073
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4074
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4076
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4077
Product: wcd9385					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCD9-220823/4078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4079
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4080
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4081
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4082
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4084
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCD9-220823/4085
Product: wcn3610					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4086
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4087
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4089
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4090
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4091
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4092
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-220823/4093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4094
Product: wcn3615					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4095
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4096
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4098
Product: wcn3620					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4099
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4100
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4101
Product: wcn3660					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	H-QUA-WCN3-220823/4102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4103
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4104
Product: wcn3660b					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4105
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4106
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/product-	H-QUA-WCN3-220823/4107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4108
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4109
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4110
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4111
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_REL	https://www.qualcomm.com/company/	H-QUA-WCN3-220823/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4113
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4114
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4116
Product: wcn3680					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4117
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4119
Product: wcn3680b					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4120
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4121
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4122
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4124
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4125
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4126
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4128
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4129
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28576		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4131
Product: wcn3910					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4132
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4133
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4134
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-220823/4135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4136
Product: wcn3950					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4137
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4138
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4139
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	H-QUA-WCN3-220823/4140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4141
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4142
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28577		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4144
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4145
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4146
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4148
Product: wcn3980					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4149
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4150
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4152
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4153
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4154
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4155
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4157
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4158
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4159
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-220823/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4161
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4162
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: wcn3988					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4164
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4165
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4166
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4167
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4169
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4170
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4171
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4173
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4174
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4175
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4177
Product: wcn3990					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4178
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4179
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-220823/4180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4181
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4182
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4183
Product: wcn3991					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4185
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4186
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4187
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4188
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4189
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-WCN3-220823/4190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: wcn3998					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4191
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4192
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4193
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4194
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-220823/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4196
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4197
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4198
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4199
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN3-220823/4200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4201
Product: wcn3999					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4202
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4203
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN3-220823/4204
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services	https://www.qualcomm.com/company/	H-QUA-WCN3-220823/4205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	product-security/bulletins/august-2023-bulletin	
Product: wcn6740					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4206
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4207
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4208
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4209
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	H-QUA-WCN6-220823/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4211
Product: wcn6750					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4212
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4213
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4215
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4216
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4217
Product: wcn6850					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4218
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN6-220823/4219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4220
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4221
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4222
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4223
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4225
Product: wcn6851					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4226
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4227
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4228
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN6-220823/4229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4230
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4231
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4232
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4233
Product: wcn6855					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	H-QUA-WCN6-220823/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4235
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4236
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4237
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4239
Product: wcn6856					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4240
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4241
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4242
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4244
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4245
Product: wcn685x-1					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4246
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4247
Product: wcn685x-5					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4248
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN6-220823/4249
Product: wcn7850					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4250
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4251
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4253
Product: wcn7851					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4254
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4255
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4256
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WCN7-220823/4257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. **CVE ID : CVE-2023-21647**	tins/august-2023-bulletin	
Product: wcn785x-1					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4258
Product: wcn785x-5					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WCN7-220823/4259
Product: wsa8810					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4260
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4262
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4263
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4264
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4265
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4266
Access of Resource Using Incompatible Type	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WSA8-220823/4267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	tins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4268
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4269
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WSA8-220823/4270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4271
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4272
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4274
Product: wsa8815					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4275
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4276
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4277
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4279
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4280
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4281
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4282
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So	https://www.qualcomm.com/company/product-security/bulle	H-QUA-WSA8-220823/4283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4284
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4285
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4286
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	H-QUA-WSA8-220823/4287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4288
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4289
Product: wsa8830					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	H-QUA-WSA8-220823/4290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4291
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4292
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4293
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4294
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666		
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4296
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4297
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4299
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4300
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4301
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4303
Product: wsa8832					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4304
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4305
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wsa8835					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4307
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4308
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4309
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4310
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4312
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4313
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4314
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4316
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4317
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4318
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	H-QUA-WSA8-220823/4320
Vendor: renault					
Product: zoe_ev_2021					
Affected Version(s): -					
N/A	03-Aug-2023	4.6	Renault Zoe EV 2021 automotive infotainment system versions 283C35202R to 283C35519R (builds 11.10.2021 to 16.01.2023) allows attackers to crash the infotainment system by sending arbitrary USB data via a USB device. **CVE ID : CVE-2023-39075**	N/A	H-REN-ZOE_-220823/4321
Vendor: Rockwellautomation					
Product: armor_powerflex					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation	08-Aug-2023	7.5	A vulnerability was discovered in the Rockwell Automation Armor PowerFlex device when the product sends communications to the local event log. Threat actors could exploit this vulnerability by sending an influx of network commands, causing the product to generate an influx of event log traffic at a high rate. If exploited, the product would stop normal operations and self-reset creating a denial-of-service condition. The error code would need to be cleared prior to resuming normal operations. **CVE ID : CVE-2023-2423**	N/A	H-ROC-ARMO-220823/4322
Vendor: ruijie					
Product: rg-ew1200g					
Affected Version(s): -					
N/A	05-Aug-2023	8.8	A vulnerability was found in Ruijie RG-EW1200G 1.0(1)B1P5. It has	N/A	H-RUI-RG-E-220823/4323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been declared as critical. Affected by this vulnerability is an unknown functionality of the file /api/sys/set_passwd of the component Administrator Password Handler. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4169**		
Vendor: Samsung					
Product: galaxy_book2_go					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go,	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	H-SAM-GALA-220823/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**		
Product: galaxy_book2_pro_360					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	H-SAM-GALA-220823/4325
Product: galaxy_book_go					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G,	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	H-SAM-GALA-220823/4326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**		
Product: galaxy_book_go_5g					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	H-SAM-GALA-220823/4327
Product: s3nrn4v					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-S3NR-220823/4328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: s3nrn82					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-S3NR-220823/4329
Product: s3nsen4					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-S3NS-220823/4330
Product: s3nsn4v					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-S3NS-220823/4331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36482		
Product: sen82ab					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-SEN8-220823/4332
Vendor: shelly					
Product: pro_4pm					
Affected Version(s): -					
Out-of-bounds Read	02-Aug-2023	5.3	Shelly 4PM Pro four-channel smart switch 0.11.0 allows an attacker to trigger a BLE out of bounds read fault condition that results in a device reload. **CVE ID : CVE-2023-33383**	N/A	H-SHE-PRO_-220823/4333
Vendor: Tenda					
Product: 4g300					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda 4G300 v1.01.42 was discovered to contain a stack overflow via the page parameter at /VirtualSer.	N/A	H-TEN-4G30-220823/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38929		
Product: ac10					
Affected Version(s): 1.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC10-220823/4335
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	H-TEN-AC10-220823/4336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-AC10-220823/4337
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC10-220823/4338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC10-220823/4339
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	H-TEN-AC10-220823/4340
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23,	N/A	H-TEN-AC10-220823/4341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: ac1206					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC12-220823/4342
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and	N/A	H-TEN-AC12-220823/4343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	H-TEN-AC12-220823/4344
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-AC12-220823/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC12-220823/4346
Product: ac5					
Affected Version(s): 1.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the	N/A	H-TEN-AC5-220823/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC5-220823/4348
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function.	N/A	H-TEN-AC5-220823/4349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38933		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	H-TEN-AC5-220823/4350
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-AC5-220823/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC5-220823/4352
Product: ac6					
Affected Version(s): 2.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC6-220823/4353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	H-TEN-AC6-220823/4354
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-AC6-220823/4355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC6-220823/4356
Product: ac7					
Affected Version(s): 1.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	H-TEN-AC7-220823/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC7-220823/4358
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	H-TEN-AC7-220823/4359
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23,	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/for	H-TEN-AC7-220823/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	mSetSpeedWan/README.md	
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC7-220823/4361
Product: ac8					
Affected Version(s): 4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-AC8-220823/4362
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	H-TEN-AC8-220823/4363
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5	N/A	H-TEN-AC8-220823/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: ac9					
Affected Version(s): 3.0					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	H-TEN-AC9-220823/4365
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were	N/A	H-TEN-AC9-220823/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	H-TEN-AC9-220823/4367
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-AC9-220823/4368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formSetSpeedWan function. **CVE ID : CVE-2023-38936**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	H-TEN-AC9-220823/4369
Product: f1202					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**	N/A	H-TEN-F120-220823/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	H-TEN-F120-220823/4371
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the mit_ssid parameter in the formWrlsafeset function. **CVE ID : CVE-2023-38939**	N/A	H-TEN-F120-220823/4372
Product: f1203					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function.	N/A	H-TEN-F120-220823/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38930		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-F120-220823/4374
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	H-TEN-F120-220823/4375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	H-TEN-F120-220823/4376
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-F120-220823/4377
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the	N/A	H-TEN-F120-220823/4378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**		
Product: fh1202					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**	N/A	H-TEN-FH12-220823/4379
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	H-TEN-FH12-220823/4380
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the mit_ssid parameter in the formWrlsafeset function.	N/A	H-TEN-FH12-220823/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38939		
Product: fh1203					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	H-TEN-FH12-220823/4382
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	H-TEN-FH12-220823/4383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	H-TEN-FH12-220823/4384
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-FH12-220823/4385
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the	N/A	H-TEN-FH12-220823/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**		
Product: fh1205					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	H-TEN-FH12-220823/4387
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function.	N/A	H-TEN-FH12-220823/4388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38933		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	H-TEN-FH12-220823/4389
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	H-TEN-FH12-220823/4390
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to	N/A	H-TEN-FH12-220823/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**		
Product: pa202					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**	N/A	H-TEN-PA20-220823/4392
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	H-TEN-PA20-220823/4393
Product: pw201a					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were	N/A	H-TEN-PW20-220823/4394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	H-TEN-PW20-220823/4395
Vendor: totolink					
Product: t10_v2					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	9.8	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setWiFiWpsConfig in /lib/cste_modules/wps.so. Attackers can send crafted data in an MQTT packet, via the pin parameter, to control the return address and execute code. **CVE ID : CVE-2023-40041**	N/A	H-TOT-T10_-220823/4396
Out-of-bounds Write	08-Aug-2023	9.8	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based	N/A	H-TOT-T10_-220823/4397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow in setStaticDhcpConfig in /lib/cste_modules/lan.so. Attackers can send crafted data in an MQTT packet, via the comment parameter, to control the return address and execute code. **CVE ID : CVE-2023-40042**		
Vendor: Tp-link					
Product: archer_ax21					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2023	9.8	TP-Link Archer AX21(US)_V3_1.1.4 Build 20230219 and AX21(US)_V3.6_1.1.4 Build 20230219 are vulnerable to Buffer Overflow. **CVE ID : CVE-2023-31710**	N/A	H-TP--ARCH-220823/4398
Vendor: unisoc					
Product: s8000					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-S800-220823/4399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-S800-220823/4400
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-S800-220823/4401
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-S800-220823/4402
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-S800-220823/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-S800-220823/4404
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-S800-220823/4405
Product: sc7731e					
Affected Version(s): -					
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-SC77-220823/4406
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	N/A	H-UNI-SC77-220823/4407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33907		
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-SC77-220823/4408
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-SC77-220823/4409
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-SC77-220823/4410
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	N/A	H-UNI-SC77-220823/4411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33912		
Product: sc9832e					
Affected Version(s): -					
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-SC98-220823/4412
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-SC98-220823/4413
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-SC98-220823/4414
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-SC98-220823/4415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33909**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-SC98-220823/4416
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-SC98-220823/4417
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-SC98-220823/4418
Product: sc9863a					
Affected Version(s): -					
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information	N/A	H-UNI-SC98-220823/4419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-SC98-220823/4420
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-SC98-220823/4421
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-SC98-220823/4422
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information	N/A	H-UNI-SC98-220823/4423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**		
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-SC98-220823/4424
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-SC98-220823/4425
Product: t310					
Affected Version(s): -					
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T310-220823/4426
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could	N/A	H-UNI-T310-220823/4427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**		
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T310-220823/4428
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T310-220823/4429
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T310-220823/4430
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead	N/A	H-UNI-T310-220823/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**		
Product: t606					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T606-220823/4432
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T606-220823/4433
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T606-220823/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T606-220823/4435
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T606-220823/4436
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T606-220823/4437
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-T606-220823/4438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T606-220823/4439
Product: t610					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T610-220823/4440
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T610-220823/4441
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no	N/A	H-UNI-T610-220823/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33907**		
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T610-220823/4443
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T610-220823/4444
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T610-220823/4445
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T610-220823/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33911**		
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T610-220823/4447
Product: t612					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T612-220823/4448
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T612-220823/4449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T612-220823/4450
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T612-220823/4451
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T612-220823/4452
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T612-220823/4453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-T612-220823/4454
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T612-220823/4455
Product: t616					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T616-220823/4456
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T616-220823/4457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33906**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T616-220823/4458
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T616-220823/4459
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T616-220823/4460
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T616-220823/4461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33910**		
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-T616-220823/4462
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T616-220823/4463
Product: t618					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T618-220823/4464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T618-220823/4465
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T618-220823/4466
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T618-220823/4467
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T618-220823/4468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T618-220823/4469
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	H-UNI-T618-220823/4470
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T618-220823/4471
Product: t760					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with	N/A	H-UNI-T760-220823/4472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed **CVE ID : CVE-2023-33913**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T760-220823/4473
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T760-220823/4474
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T760-220823/4475
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T760-220823/4476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33909**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T760-220823/4477
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T760-220823/4478
Product: t770					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T770-220823/4479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	H-UNI-T770-220823/4480
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T770-220823/4481
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T770-220823/4482
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T770-220823/4483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	H-UNI-T770-220823/4484
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T770-220823/4485
Product: t820					
Affected Version(s): -					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	H-UNI-T820-220823/4486
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T820-220823/4487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33906**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	H-UNI-T820-220823/4488
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	H-UNI-T820-220823/4489
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	H-UNI-T820-220823/4490
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	H-UNI-T820-220823/4491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33910**		
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	H-UNI-T820-220823/4492
Operating System					
Vendor: ABB					
Product: ac700f_firmware					
Affected Version(s): 9.2.0					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible.	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-AC70-220823/4493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects:	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-AC70-220823/4494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0426**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-AC70-220823/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-	O-ABB-AC70-220823/4496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1;	1911411808. 1686627590	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0426**		
Product: freelance_2013					
Affected Version(s): -					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-FREE-220823/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-FREE-220823/4498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0426		
Product: freelance_2016					
Affected Version(s): -					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F:	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-FREE-220823/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=L	O-ABB-FREE-220823/4500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1;	aunch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0426**		
Product: freelance_2019					
Affected Version(s): -					
Numeric Range Comparison Without Minimum Check	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-FREE-220823/4501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities could cause the product to stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1. **CVE ID : CVE-2023-0425**		
Stack-based Buffer Overflow	07-Aug-2023	7.5	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007517&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.68514131.339223974.1691382343-1911411808.1686627590	O-ABB-FREE-220823/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0426		
Vendor: Advantech					
Product: eki-1521_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**	N/A	O-ADV-EKI--220823/4503
Affected Version(s): * Up to (including) 1.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface. **CVE ID : CVE-2023-4203**	N/A	O-ADV-EKI--220823/4504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: eki-1522_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**	N/A	O-ADV-EKI--220823/4505
Affected Version(s): * Up to (including) 1.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface. **CVE ID : CVE-2023-4203**	N/A	O-ADV-EKI--220823/4506
Product: eki-1524_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Input	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a	N/A	O-ADV-EKI--220823/4507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface. **CVE ID : CVE-2023-4202**		
Affected Version(s): * Up to (including) 1.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	5.4	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface. **CVE ID : CVE-2023-4203**	N/A	O-ADV-EKI--220823/4508
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	04-Aug-2023	9.1	An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-	https://kb.nomachine.com/TR07U10948	O-APP-MACO-220823/4509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			owned files by using hardlinks. **CVE ID : CVE-2023-39107**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2023	8.8	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4073**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	O-APP-MACO-220823/4510
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4511
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	O-APP-MACO-220823/4512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38231**	ts/acrobat/apsb23-30.html	
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38234**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4514
Use After Free	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 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-2023-38211**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	O-APP-MACO-220823/4515
Heap-based Buffer Overflow	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 is affected by a Heap-based Buffer Overflow	https://helpx.adobe.com/security/products/dimension/	O-APP-MACO-220823/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38212**	apsb23-44.html	
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38222**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4517
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38223**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4519
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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/acrobat/apsb23-30.html	O-APP-MACO-220823/4520

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-2023-38225**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4521
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38227**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38228**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4523
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38246**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from 4.0.0 through 4.0.2, from 3.1.0 through 3.1.27. **CVE ID : CVE-2023-4136**	N/A	O-APP-MACO-220823/4525
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29303**		
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**	https://my.f5.com/manage/s/article/K000132563	O-APP-MACO-220823/4527
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38235**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4529
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4530

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-2023-38236**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38237**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4531
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38238**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38239**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4533
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38240**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38241**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4535
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38242**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38243**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4537
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	O-APP-MACO-220823/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30467 (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-2023-38244**	ts/acrobat/apsb23-30.html	
Exposure of Sensitive Information to an Unauthorized Actor	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38245		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38230**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4540
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38247**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38248**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4542
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38229**		
Out-of-bounds Read	09-Aug-2023	5.5	Adobe Dimension version 3.4.9 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-2023-38213**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	O-APP-MACO-220823/4544
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-APP-MACO-220823/4545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**		
Vendor: assmann					
Product: ht-ip211hdp_firmware					
Affected Version(s): 2.000.022					
Cleartext Storage of Sensitive Information	04-Aug-2023	7.5	Assmann Digitus Plug&View IP Camera HT-IP211HDP, version 2.000.022 allows unauthenticated attackers to download a copy of the camera's settings and the administrator credentials. **CVE ID : CVE-2023-30146**	N/A	O-ASS-HT-I-220823/4546
Vendor: Asus					
Product: rt-ac66u_b1_firmware					
Affected Version(s): 3.0.0.4.286_51665					
Cleartext Transmission of Sensitive Information	08-Aug-2023	7.5	ASUS RT-AC66U B1 3.0.0.4.286_51665 was discovered to transmit sensitive information in cleartext. **CVE ID : CVE-2023-39086**	N/A	O-ASU-RT-A-220823/4547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Broadcom					
Product: brocade_fabric_operating_system					
Affected Version(s): 9.2.0					
Improper Privilege Management	02-Aug-2023	7.8	Through manipulation of passwords or other variables, using commands such as portcfgupload, configupload, license, myid, a non-privileged user could obtain root privileges in Brocade Fabric OS versions before Brocade Fabric OS v9.1.1c and v9.2.0. **CVE ID : CVE-2023-31432**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22385	O-BRO-BROC-220823/4548
Unrestricted Upload of File with Dangerous Type	02-Aug-2023	5.5	Brocade Fabric OS before Brocade Fabric OS v9.1.1c, v9.2.0 contains a vulnerability in the command line that could allow a local user to dump files under user's home directory using grep. **CVE ID : CVE-2023-31428**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22380	O-BRO-BROC-220823/4549
Affected Version(s): * Up to (excluding) 9.1.1c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Aug-2023	7.8	Through manipulation of passwords or other variables, using commands such as portcfgupload, configupload, license, myid, a non-privileged user could obtain root privileges in Brocade Fabric OS versions before Brocade Fabric OS v9.1.1c and v9.2.0. **CVE ID : CVE-2023-31432**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22385	O-BRO-BROC-220823/4550
Improper Initialization	02-Aug-2023	7.1	System files could be overwritten using the less command in Brocade Fabric OS before Brocade Fabric OS v9.1.1c and v9.2.0. **CVE ID : CVE-2023-31926**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22388	O-BRO-BROC-220823/4551
Unrestricted Upload of File with Dangerous Type	02-Aug-2023	5.5	Brocade Fabric OS before Brocade Fabric OS v9.1.1c, v9.2.0 contains a vulnerability in the command line that could allow a local user to dump files	https://support.broadcom.com/external/content/SecurityAdvisories/0/22380	O-BRO-BROC-220823/4552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under user's home directory using grep. **CVE ID : CVE-2023-31428**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-2023	5.5	A buffer overflow vulnerability in "secpolicydelete" command in Brocade Fabric OS before Brocade Fabric OS v9.1.1c and v9.2.0 could allow an authenticated privileged user to crash the Brocade Fabric OS switch leading to a denial of service. **CVE ID : CVE-2023-31430**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22381	O-BRO-BROC-220823/4553
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-2023	5.5	A buffer overflow vulnerability in "diagstatus" command in Brocade Fabric OS before Brocade Fabric v9.2.0 and v9.1.1c could allow an authenticated user to crash the Brocade Fabric OS switch leading to a denial of service.	https://support.broadcom.com/external/content/SecurityAdvisories/0/22384	O-BRO-BROC-220823/4554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31431		
N/A	02-Aug-2023	5.3	An information disclosure in the web interface of Brocade Fabric OS versions before Brocade Fabric OS v9.2.0 and v9.1.1c, could allow a remote unauthenticated attacker to get technical details about the web interface. **CVE ID : CVE-2023-31927**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22389	O-BRO-BROC-220823/4555
Affected Version(s): * Up to (excluding) 9.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	6.1	A reflected cross-site scripting (XSS) vulnerability exists in Brocade Webtools PortSetting.html of Brocade Fabric OS version before Brocade Fabric OS v9.2.0 that could allow a remote unauthenticated attacker to execute arbitrary JavaScript code in a target user's session with the Brocade	https://support.broadcom.com/external/content/SecurityAdvisories/0/22390	O-BRO-BROC-220823/4556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Webtools application. **CVE ID : CVE-2023-31928**		
Product: fabric_operating_system					
Affected Version(s): * Up to (excluding) 9.1.1c					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2023	7.8	Brocade Fabric OS versions before Brocade Fabric OS v9.1.1c, and v9.2.0 Could allow an authenticated, local user with knowledge of full path names inside Brocade Fabric OS to execute any command regardless of assigned privilege. Starting with Fabric OS v9.1.0, “root” account access is disabled. **CVE ID : CVE-2023-31427**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22379	O-BRO-FABR-220823/4557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	5.5	Brocade Fabric OS before Brocade Fabric OS v9.1.1c, v9.2.0 contains a vulnerability when using various commands such as “chassisdistribute”, “reboot”, “rasman”, errmoduleshow, errfilterset, hassiscfgperrthreshold, supportshowcfgdisable and supportshowcfgenable commands that can cause the content of shell interpreted variables to be printed in the terminal. **CVE ID : CVE-2023-31429**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22408	O-BRO-FABR-220823/4558
Affected Version(s): * Up to (excluding) 8.2.3d					
Insertion of Sensitive Information into Log File	01-Aug-2023	6.5	The Brocade Fabric OS Commands “configupload” and “configdownload” before Brocade Fabric OS v9.1.1c, v8.2.3d, v9.2.0 print scp, sftp, ftp servers passwords in supportsave. This	N/A	O-BRO-FABR-220823/4559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow a remote authenticated attacker to access sensitive information. **CVE ID : CVE-2023-31426**		
Affected Version(s): 9.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Aug-2023	7.8	A vulnerability in the fosexec command of Brocade Fabric OS after Brocade Fabric OS v9.1.0 and, before Brocade Fabric OS v9.1.1 could allow a local authenticated user to perform privilege escalation to root by breaking the rbash shell. Starting with Fabric OS v9.1.0, “root” account access is disabled. **CVE ID : CVE-2023-31425**	https://support.broadcom.com/external/content/SecurityAdvisories/0/22407	O-BRO-FABR-220823/4560
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.1.1c					
Insertion of Sensitive Informatio	01-Aug-2023	6.5		N/A	O-BRO-FABR-220823/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			The Brocade Fabric OS Commands “configupload” and “configdownload” before Brocade Fabric OS v9.1.1c, v8.2.3d, v9.2.0 print scp, sftp, ftp servers passwords in supportsave. This could allow a remote authenticated attacker to access sensitive information. **CVE ID : CVE-2023-31426**		
Vendor: Cisco					
Product: asyncos					
Affected Version(s): 11.7.0-406					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.7.0-418					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.7.1-006					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.7.1-020					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.7.1-049					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.7.2-011					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.8.0-414					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.8.1-023					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.8.3-018					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 11.8.3-021					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.0.1-268					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.0.3-007					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.5.1-011					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.5.2-007					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.5.4-005					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 12.5.5-004					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.0.2-012					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.0.3-014					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.0.4-005					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.5.0-498					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.5.1-008					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Affected Version(s): 14.5.1-016					
N/A	03-Aug-2023	5.3	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj	O-CIS-ASYN-220823/4583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device. **CVE ID : CVE-2023-20215**		
Product: spa500ds_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa500s_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa501g_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa502g_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa504g_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-	O-CIS-SPA5-220823/4592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	multi-7kvPmu2F	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}]] **CVE ID : CVE-2023-20218**		
Product: spa508g_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-	O-CIS-SPA5-220823/4594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	multi-7kvPmu2F	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}]] **CVE ID : CVE-2023-20218**		
Product: spa509g_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SPA5-220823/4596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	o-sa-spa-web-multi-7kvPmu2F	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa512g_firmware					
Affected Version(s): -					
Improper Neutralization of Input	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-SPA5-220823/4598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa514g_firmware					
Affected Version(s): -					
Improper Neutralization of	03-Aug-2023	6.1	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com/security/c	O-CIS-SPA5-220823/4600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	enter/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**		
Product: spa525g2_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4602
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"]}}]] **CVE ID : CVE-2023-20218**		
Product: spa525g_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4604
Improper Neutralization of Input During Web Page Generation	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-	O-CIS-SPA5-220823/4605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]] **CVE ID : CVE-2023-20218**	multi-7kvPmu2F	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: spa525_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20181**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-multi-7kvPmu2F	O-CIS-SPA5-220823/4606
Improper Neutralization of Input During Web Page Generation	03-Aug-2023	6.1	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-web-	O-CIS-SPA5-220823/4607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]]	multi-7kvPmu2F	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20218		
Vendor: connectedio					
Product: er2000t-vz-cat1_firmware					
Affected Version(s): * Up to (including) 2.1.0					
N/A	04-Aug-2023	9.8	Connected IO v2.1.0 and prior has a misconfiguration in their MQTT broker used for management and device communication, which allows devices to connect to the broker and issue commands to other device, impersonating Connected IO management platform and sending commands to all of Connected IO's devices. **CVE ID : CVE-2023-33379**	N/A	O-CON-ER20-220823/4608
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.	O-DEB-DEBI-220823/4609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	mozilla.org/security/advisories/mfsa2023-29/	
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4610
Affected Version(s): 11.0					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisor	O-DEB-DEBI-220823/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	ies/mfsa2023-29/	
N/A	01-Aug-2023	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4047**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4612
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2023	8.8	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4073**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	O-DEB-DEBI-220823/4613
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with	https://www.mozilla.org/security/advisories/mfsa2023-30/,	O-DEB-DEBI-220823/4614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Out-of-bounds Write	01-Aug-2023	7.5	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4050**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4615
N/A	01-Aug-2023	7.5	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14,	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Firefox ESR < 115.1. **CVE ID : CVE-2023-4055**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2023	5.9	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4049**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4617
Origin Validation Error	01-Aug-2023	5.3	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4045**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4618
N/A	01-Aug-2023	5.3	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis.	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.	O-DEB-DEBI-220823/4619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4046**	mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Affected Version(s): 12.0					
Out-of-bounds Write	01-Aug-2023	9.8	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4056**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4620
N/A	01-Aug-2023	8.8	A bug in popup notifications delay calculation could have made it possible for an	https://www.mozilla.org/security/advisories/mfsa2023-30/,	O-DEB-DEBI-220823/4621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4047**	https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2023	8.8	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4073**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	O-DEB-DEBI-220823/4622
Out-of-bounds Read	01-Aug-2023	7.5	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4048**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4623
Out-of-bounds Write	01-Aug-2023	7.5	In some cases, an untrusted input stream was copied to	https://www.mozilla.org/security/advisor	O-DEB-DEBI-220823/4624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4050**	ies/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	
N/A	01-Aug-2023	7.5	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4055**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4625
Concurrent Execution using Shared Resource with Improper Synchronization	01-Aug-2023	5.9	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/,	O-DEB-DEBI-220823/4626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4049**	https://www.mozilla.org/security/advisories/mfsa2023-29/	
Origin Validation Error	01-Aug-2023	5.3	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4045**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4627
N/A	01-Aug-2023	5.3	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1. **CVE ID : CVE-2023-4046**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/	O-DEB-DEBI-220823/4628
Vendor: Emerson					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dl8000_firmware					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	O-EME-DL80-220823/4629
Product: roc809l_firmware					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	O-EME-ROC8-220823/4630
Product: roc809_firmware					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device	N/A	O-EME-ROC8-220823/4631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**		
Product: roc827l_firmware					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	O-EME-ROC8-220823/4632
Product: roc827_firmware					
Affected Version(s): *					
Improper Authentication	02-Aug-2023	9.4	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition. **CVE ID : CVE-2023-1935**	N/A	O-EME-ROC8-220823/4633
Vendor: Epson					
Product: ep-801a_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation	https://www.epson.jp/supp	O-EPS-EP-8-220823/4634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	ort/misc_t/230802_oshirase.htm	
Product: ep-802a_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-EP-8-220823/4635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: ep-901a_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-EP-9-220823/4636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: ep-901f_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-EP-9-220823/4637
Product: ep-902a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-EP-9-220823/4638
Product: pa-tcu1_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer.	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PA-T-220823/4639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: pm-t960_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PM-T-220823/4640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: pm-t990_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor.	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PM-T-220823/4641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38556		
Product: px-201_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PX-2-220823/4642
Product: px-502a_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PX-5-220823/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: px-601f_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PX-6-220823/4644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. **CVE ID : CVE-2023-38556**		
Product: px-602f_firmware					
Affected Version(s): -					
N/A	02-Aug-2023	7.5	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the	https://www.epson.jp/support/misc_t/230802_oshirase.htm	O-EPS-PX-6-220823/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information provided by the vendor. **CVE ID : CVE-2023-38556**		
Vendor: ezviz					
Product: cs-c6n-a0-1c2wfr-mul_firmware					
Affected Version(s): * Up to (including) 5.3.2					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-c6n-b0-1g2wf_firmware					
Affected Version(s): * Up to (including) 5.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-c6n-r101-1g2wf_firmware					
Affected Version(s): * Up to (including) 5.3.0					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34552		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv248-a0-32wmfr_firmware					
Affected Version(s): * Up to (including) 5.2.3					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34551		
Product: cs-cv310-a0-1b2wfr_firmware					
Affected Version(s): * Up to (including) 5.3.0					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-1c2wfr-c_firmware					
Affected Version(s): * Up to (including) 5.3.2					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-1c2wfr_firmware					
Affected Version(s): * Up to (including) 5.3.2					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command	https://www.ezviz.com/data-security/security-	O-EZV-CS-C-220823/4659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C	notice/detail/827	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: cs-cv310-a0-3c2wfrl-1080p_firmware					
Affected Version(s): * Up to (including) 5.2.7					
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-CS-C-220823/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Product: lc1c_firmware					
Affected Version(s): * Up to (including) 5.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2023	8.8	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-LC1C-220823/4662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. **CVE ID : CVE-2023-34552**		
Out-of-bounds Write	01-Aug-2023	8	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before	https://www.ezviz.com/data-security/security-notice/detail/827	O-EZV-LC1C-220823/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote). **CVE ID : CVE-2023-34551**		
Vendor: F5					
Product: big-ip_10200v-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_10350v-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_11000-f_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_11050-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Product: big-ip_5250v-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_6900-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_7200v-f_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_8900-f_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_i15820-df_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the	https://my.f5.com/manage/s/article/K00135449	O-F5-BIG--220823/4672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3470		
Product: big-ip_i5820-df_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Product: big-ip_i7820-df_firmware					
Affected Version(s): -					
Weak Password Requirements	02-Aug-2023	6.1	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User	https://my.f5.com/manage/s/article/K000135449	O-F5-BIG--220823/4674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-3470**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): -					
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4132**	https://access.redhat.com/security/cve/CVE-2023-4132	O-FED-FEDO-220823/4675
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a	https://access.redhat.com/security/cve/CVE-2023-4133	O-FED-FEDO-220823/4676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible rearming of the flower_stats_timer from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4133**		
Affected Version(s): 37					
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate.	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-3-lersek@redhat.com/	O-FED-FEDO-220823/4677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4194		
Affected Version(s): 38					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-2023	8.8	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-4073**	https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop.html	O-FED-FEDO-220823/4678
Use After Free	07-Aug-2023	7.8	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system. **CVE ID : CVE-2023-4147**	https://access.redhat.com/security/cve/CVE-2023-4147, https://www.spinics.net/lists/stable/msg671573.html, https://bugzilla.redhat.com/show_bug.cgi?id=2225239	O-FED-FEDO-220823/4679
Insecure Preserved Inherited Permissions	04-Aug-2023	7.3	Cargo downloads the Rust project's dependencies and compiles the project. Cargo prior to version 0.72.2, bundled with Rust prior to version 1.71.1, did not respect the umask when extracting	https://github.com/rust-lang/cargo/pull/12443, https://github.com/rust-lang/cargo/commit/d78bbf4bde3c6b95caca7512f537c6f9721426ff,	O-FED-FEDO-220823/4680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crate archives on UNIX-like systems. If the user downloaded a crate containing files writeable by any local user, another local user could exploit this to change the source code compiled and executed by the current user. To prevent existing cached extractions from being exploitable, the Cargo binary version 0.72.2 included in Rust 1.71.1 or later will purge caches generated by older Cargo versions automatically. As a workaround, configure one's system to prevent other local users from accessing the Cargo directory, usually located in `~/.cargo`. **CVE ID : CVE-2023-38497**	https://github.com/rust-lang/cargo/security/advisories/GHSA-j3xp-wfr4-hx87	
Out-of-bounds Read	04-Aug-2023	6.5	A heap out-of-bounds memory read flaw was found in the virtual nvme device in QEMU. The QEMU process does not validate an offset provided by the guest before computing a host	https://bugzilla.redhat.com/show_bug.cgi?id=2229101	O-FED-FEDO-220823/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap pointer, which is used for copying data back to the guest. Arbitrary heap memory relative to an allocated buffer can be disclosed. **CVE ID : CVE-2023-4135**		
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate. **CVE ID : CVE-2023-4194**	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-3-lersek@redhat.com/	O-FED-FEDO-220823/4682
Vendor: Freebsd					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: freebsd					
Affected Version(s): 12.4					
Integer Overflow or Wraparound	01-Aug-2023	7.5	A set of carefully crafted ipv6 packets can trigger an integer overflow in the calculation of a fragment reassembled packet's payload length field. This allows an attacker to trigger a kernel panic, resulting in a denial of service. **CVE ID : CVE-2023-3107**	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:06.ipv6.asc	O-FRE-FREE-220823/4683
Affected Version(s): 13.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Aug-2023	8.8	The fwctl driver implements a state machine which is executed when a bhyve guest accesses certain x86 I/O ports. The interface lets the guest copy a string into a buffer resident in the bhyve process' memory. A bug in the state machine implementation can result in a buffer overflowing when copying this string. Malicious, privileged software running in a guest VM can exploit the buffer overflow to achieve code execution on the host in the bhyve	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:07.bhyve.asc	O-FRE-FREE-220823/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			userspace process, which typically runs as root, mitigated by the capabilities assigned through the Capsicum sandbox available to the bhyve process. **CVE ID : CVE-2023-3494**		
Integer Overflow or Wraparound	01-Aug-2023	7.5	A set of carefully crafted ipv6 packets can trigger an integer overflow in the calculation of a fragment reassembled packet's payload length field. This allows an attacker to trigger a kernel panic, resulting in a denial of service. **CVE ID : CVE-2023-3107**	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:06.ipv6.asc	O-FRE-FREE-220823/4685
Affected Version(s): 13.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Aug-2023	8.8	The fwctl driver implements a state machine which is executed when a bhyve guest accesses certain x86 I/O ports. The interface lets the guest copy a string into a buffer resident in the bhyve process' memory. A bug in the state machine implementation can result in a buffer overflowing when	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:07.bhyve.asc	O-FRE-FREE-220823/4686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copying this string. Malicious, privileged software running in a guest VM can exploit the buffer overflow to achieve code execution on the host in the bhyve userspace process, which typically runs as root, mitigated by the capabilities assigned through the Capsicum sandbox available to the bhyve process. **CVE ID : CVE-2023-3494**		
Integer Overflow or Wraparound	01-Aug-2023	7.5	A set of carefully crafted ipv6 packets can trigger an integer overflow in the calculation of a fragment reassembled packet's payload length field. This allows an attacker to trigger a kernel panic, resulting in a denial of service. **CVE ID : CVE-2023-3107**	https://security.FreeBSD.org/advisories/FreeBSD-SA-23:06.ipv6.asc	O-FRE-FREE-220823/4687
Vendor: gatesair					
Product: flexiva_fax_150w_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Aug-2023	9.8	An isssue in GatesAIr Flexiva FM Transmitter/Exiter Fax 150W allows a remote attacker to gain privileges via	N/A	O-GAT-FLEX-220823/4688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the LDAP and SMTP credentials. **CVE ID : CVE-2023-36082**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2023	5.4	Cross Site Scripting vulnerability in GatesAIr Flexiva FM Transmitter/Exciter v.FAX 150W allows a remote attacker to execute arbitrary code via a crafted script to the web application dashboard. **CVE ID : CVE-2023-36081**	N/A	O-GAT-FLEX-220823/4689
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	01-Aug-2023	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 115.0.5790.98 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-3736**	https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-desktop.html, https://crbug.com/1434438	O-GOO-ANDR-220823/4690
Affected Version(s): 10.0					
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-	O-GOO-ANDR-220823/4691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4692
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	O-GOO-ANDR-220823/4693
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information	https://corp.mediatek.com	O-GOO-ANDR-220823/4694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	/product-security-bulletin/August-2023	
Affected Version(s): 11.0					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	O-GOO-ANDR-220823/4695
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4697
Out-of-bounds Write	07-Aug-2023	6.7	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. **CVE ID : CVE-2023-20808**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. **CVE ID : CVE-2023-20809**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4699
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4700
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	O-GOO-ANDR-220823/4701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33906**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	O-GOO-ANDR-220823/4702
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33908**	N/A	O-GOO-ANDR-220823/4703
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	O-GOO-ANDR-220823/4704
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no	N/A	O-GOO-ANDR-220823/4705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges **CVE ID : CVE-2023-33910**		
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	O-GOO-ANDR-220823/4706
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	O-GOO-ANDR-220823/4707
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20780		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4709
Affected Version(s): 12.0					
Out-of-bounds Write	07-Aug-2023	7.2	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed **CVE ID : CVE-2023-33913**	N/A	O-GOO-ANDR-220823/4710
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**		
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4712
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905;	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**		
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4714
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4716
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4717
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4719
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560;	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**		
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4721
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4723
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4724
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**		
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4726
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524;	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4728
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735. **CVE ID : CVE-2023-20788**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4729
Use After Free	07-Aug-2023	6.4	In thermal, there is a possible use after free due to a race condition. This could	https://corp.mediatek.com/product-security-	O-GOO-ANDR-220823/4730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734. **CVE ID : CVE-2023-20787**	bulletin/August-2023	
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**	N/A	O-GOO-ANDR-220823/4731
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	O-GOO-ANDR-220823/4732
Missing Authorization	07-Aug-2023	5.5	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	N/A	O-GOO-ANDR-220823/4733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33908		
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	O-GOO-ANDR-220823/4734
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	O-GOO-ANDR-220823/4735
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	O-GOO-ANDR-220823/4736
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4738
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20798		
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4740
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4741
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4743
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**		
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4745
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 13.0					
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. **CVE ID : CVE-2023-20816**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4747
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587. **CVE ID : CVE-2023-20815**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4748
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	O-GOO-ANDR-220823/4749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905. **CVE ID : CVE-2023-20783**	bulletin/August-2023	
Out-of-bounds Write	07-Aug-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989. **CVE ID : CVE-2023-20784**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4750
Out-of-bounds Write	07-Aug-2023	6.7	In gps, 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	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811. **CVE ID : CVE-2023-20786**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. **CVE ID : CVE-2023-20814**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4752
Out-of-bounds Write	07-Aug-2023	6.7	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433. **CVE ID : CVE-2023-20807**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	6.7	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437. **CVE ID : CVE-2023-20806**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4754
Out-of-bounds Write	07-Aug-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900. **CVE ID : CVE-2023-20795**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4755
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411. **CVE ID : CVE-2023-20805**		
Out-of-bounds Write	07-Aug-2023	6.7	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582. **CVE ID : CVE-2023-20797**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4757
Out-of-bounds Write	07-Aug-2023	6.7	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07199773; Issue ID: ALPS07326384. **CVE ID : CVE-2023-20804**		
Out-of-bounds Write	07-Aug-2023	6.7	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. **CVE ID : CVE-2023-20817**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4759
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374. **CVE ID : CVE-2023-20803**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Aug-2023	6.5	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955. **CVE ID : CVE-2023-20800**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4761
Out-of-bounds Write	07-Aug-2023	6.5	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976. **CVE ID : CVE-2023-20802**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4762
Out-of-bounds Write	07-Aug-2023	6.4	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524. **CVE ID : CVE-2023-20785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-Aug-2023	6.4	In imgsys, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968. **CVE ID : CVE-2023-20801**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4764
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33912**	N/A	O-GOO-ANDR-220823/4765
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information	N/A	O-GOO-ANDR-220823/4766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with no additional execution privileges **CVE ID : CVE-2023-33906**		
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33907**	N/A	O-GOO-ANDR-220823/4767
Missing Authorization	07-Aug-2023	5.5	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33909**	N/A	O-GOO-ANDR-220823/4768
Missing Authorization	07-Aug-2023	5.5	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33910**	N/A	O-GOO-ANDR-220823/4769
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This	https://corp.mediatek.com/product-security-	O-GOO-ANDR-220823/4770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549. **CVE ID : CVE-2023-20813**	bulletin/August-2023	
N/A	07-Aug-2023	4.4	In jpeg, there is a possible information disclosure 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. Patch ID: ALPS07693193; Issue ID: ALPS07693193. **CVE ID : CVE-2023-20789**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4771
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103. **CVE ID : CVE-2023-20782**		
Out-of-bounds Write	07-Aug-2023	4.4	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323. **CVE ID : CVE-2023-20781**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4773
Out-of-bounds Read	07-Aug-2023	4.4	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076. **CVE ID : CVE-2023-20798**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-2023	4.4	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540. **CVE ID : CVE-2023-20818**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4775
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4776
Out-of-bounds Write	07-Aug-2023	4.4	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818. **CVE ID : CVE-2023-20793**		
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4778
Out-of-bounds Write	07-Aug-2023	4.4	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987;	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07944987. **CVE ID : CVE-2023-20812**		
N/A	07-Aug-2023	4.4	In keyinstall, there is a possible information disclosure 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. Patch ID: ALPS08017756; Issue ID: ALPS08017756. **CVE ID : CVE-2023-20780**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-GOO-ANDR-220823/4780
Affected Version(s): 9.0					
Missing Authorization	07-Aug-2023	5.5	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges **CVE ID : CVE-2023-33911**	N/A	O-GOO-ANDR-220823/4781
Product: chrome_os					
Affected Version(s): -					
Use After Free	01-Aug-2023	8.8	Use after free in Splitscreen in Google Chrome on ChromeOS prior to 115.0.5790.131	https://crbug.com/1451803	O-GOO-CHRO-220823/4782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. (Chromium security severity: High) **CVE ID : CVE-2023-3729**		
Use After Free	01-Aug-2023	8.8	Use after free in Diagnostics in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) **CVE ID : CVE-2023-3731**	https://crbug.com/1441306, https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-chromeos.html	O-GOO-CHRO-220823/4783
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	6.3	Insufficient validation of untrusted input in Chromad in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker to execute arbitrary code via a crafted shell script.	https://crbug.com/1398986, https://chromereleases.googleblog.com/2023/07/stable-channel-update-for-chromeos.html	O-GOO-CHRO-220823/4784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Low) **CVE ID : CVE-2023-3739**		
Vendor: hpe					
Product: arubaos-cx					
Affected Version(s): From (including) 10.10.0000 Up to (including) 10.10.1050					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	O-HPE-ARUB-220823/4785
Affected Version(s): From (including) 10.11.0000 Up to (including) 10.11.1010					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Aug-2023	8.8	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-010.txt	O-HPE-ARUB-220823/4786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX. **CVE ID : CVE-2023-3718**		
Vendor: Insyde					
Product: kernel					
Affected Version(s): From (including) 5.0 Up to (including) 5.5					
Incorrect Authorization	03-Aug-2023	6.5	An issue was discovered in FvbServicesRuntimeDxe in Insyde InsydeH2O with kernel 5.0 through 5.5. The FvbServicesRuntimeDxe SMM module exposes an SMI handler that allows an attacker to interact with the SPI flash at run-time from the OS. **CVE ID : CVE-2023-28468**	https://www.insyde.com/security-pledge/SA-2023039	O-INS-KERN-220823/4787
Vendor: Johnsoncontrols					
Product: videoedge					
Affected Version(s): * Up to (excluding) 6.1.1					
Insufficient Verification of Data	03-Aug-2023	5.5	A local user could edit the VideoEdge configuration file	https://www.johnsoncontrols.com/cyber-	O-JOH-VIDE-220823/4788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			and interfere with VideoEdge operation. **CVE ID : CVE-2023-3749**	solutions/security-advisories	
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	08-Aug-2023	7.8	Insufficient validation in the IOCTL (Input Output Control) input buffer in AMD uProf may allow an authenticated user to load an unsigned driver potentially leading to arbitrary kernel execution. **CVE ID : CVE-2023-20562**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-LIN-LINU-220823/4789
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from 4.0.0 through 4.0.2, from 3.1.0 through 3.1.27. **CVE ID : CVE-2023-4136**	N/A	O-LIN-LINU-220823/4790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary buffer potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20556**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-LIN-LINU-220823/4791
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary address potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20561**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-LIN-LINU-220823/4792
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a possible rearming of the flower_stats_timer	https://access.redhat.com/security/cve/CVE-2023-4133	O-LIN-LINU-220823/4793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4133**		
Affected Version(s): * Up to (excluding) 6.5					
Use After Free	07-Aug-2023	7.8	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system. **CVE ID : CVE-2023-4147**	https://access.redhat.com/security/cve/CVE-2023-4147, https://www.spinics.net/lists/stable/msg671573.html, https://bugzilla.redhat.com/show_bug.cgi?id=2225239	O-LIN-LINU-220823/4794
Affected Version(s): * Up to (including) 6.2.16					
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4132**	https://access.redhat.com/security/cve/CVE-2023-4132	O-LIN-LINU-220823/4795
Affected Version(s): * Up to (including) 6.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate. **CVE ID : CVE-2023-4194**	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-3-lersek@redhat.com/	O-LIN-LINU-220823/4796
Affected Version(s): 4.19					
Out-of-bounds Write	07-Aug-2023	6.7	In IOMMU, 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.	https://corp.mediatek.com/product-security-bulletin/August-2023	O-LIN-LINU-220823/4797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20811**		
N/A	07-Aug-2023	4.4	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061. **CVE ID : CVE-2023-20810**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-LIN-LINU-220823/4798
Affected Version(s): 6.5					
Use After Free	07-Aug-2023	7.8	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system. **CVE ID : CVE-2023-4147**	https://access.redhat.com/security/cve/CVE-2023-4147, https://www.spinics.net/lists/stable/msg671573.html, https://bugzilla.redhat.com/show_bug.cgi?id=2225239	O-LIN-LINU-220823/4799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate. **CVE ID : CVE-2023-4194**	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-3-lersek@redhat.com/	O-LIN-LINU-220823/4800
Vendor: mi					
Product: xiaomi_router_firmware					
Affected Version(s): * Up to (excluding) 2023.2					
Improper Neutralization of Special Elements used in a Command	02-Aug-2023	9.8	A vulnerability has been discovered in Xiaomi routers that could allow command injection through an external interface. This	https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=529	O-MI-XIAO-220823/4801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			vulnerability arises from inadequate filtering of responses returned from the external interface. Attackers could exploit this vulnerability by hijacking the ISP or an upper-layer router to gain privileges on the Xiaomi router. Successful exploitation of this flaw could permit remote code execution and complete compromise of the device. **CVE ID : CVE-2023-26317**		
Vendor: Microsoft					
Product: azure_devops_server					
Affected Version(s): 2019.0.1					
N/A	08-Aug-2023	6.3	Azure DevOps Server Spoofing Vulnerability **CVE ID : CVE-2023-36869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36869	O-MIC-AZUR-220823/4802
Affected Version(s): 2019.1.2					
N/A	08-Aug-2023	6.3	Azure DevOps Server Spoofing Vulnerability **CVE ID : CVE-2023-36869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36869	O-MIC-AZUR-220823/4803
Affected Version(s): 2020.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.3	Azure DevOps Server Spoofing Vulnerability **CVE ID : CVE-2023-36869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36869	O-MIC-AZUR-220823/4804
Affected Version(s): 2022.0.1					
N/A	08-Aug-2023	6.3	Azure DevOps Server Spoofing Vulnerability **CVE ID : CVE-2023-36869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36869	O-MIC-AZUR-220823/4805
Product: windows					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2023	9.8	PaperCut NG and PaperCut MF before 22.1.3 on Windows allow path traversal, enabling attackers to upload, read, or delete arbitrary files. This leads to remote code execution when external device integration is enabled (a very common configuration). **CVE ID : CVE-2023-39143**	https://www.papercut.com/kb/Main/securitybulletinjuly2023/	O-MIC-WIND-220823/4806
N/A	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29320**		
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38226**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4808
N/A	08-Aug-2023	7.8	Insufficient validation in the IOCTL (Input Output Control) input buffer in AMD uProf may	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-MIC-WIND-220823/4809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated user to load an unsigned driver potentially leading to arbitrary kernel execution. **CVE ID : CVE-2023-20562**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38227**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4810
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38228**		
Heap-based Buffer Overflow	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 is affected by a Heap-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-2023-38212**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	O-MIC-WIND-220823/4812
N/A	03-Aug-2023	7.8	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator. **CVE ID : CVE-2023-32764**	https://help.supportservices.fabasoft.com/index.php?topic=doc/Vulnerabilities-Fabasoft-Folio/vulnerabilities-2023.htm#client-autoupdate-harmful-code-installation-vulnerability-pdo06614-	O-MIC-WIND-220823/4813
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and	https://helpx.adobe.com/security/produc	O-MIC-WIND-220823/4814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30467 (and earlier) are 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-2023-38246**	ts/acrobat/apsb23-30.html	
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38231**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4815
Use After Free	09-Aug-2023	7.8	Adobe Dimension version 3.4.9 is affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/dimension/	O-MIC-WIND-220823/4816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38211**	apsb23-44.html	
Out-of-bounds Write	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38233**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4817
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38234**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38222**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4819
Access of Uninitialized Pointer	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4820

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-2023-38223**		
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38224**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4821
Use After Free	10-Aug-2023	7.8	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38225**		
Incorrect Authorization	07-Aug-2023	7.5	The event analysis component in Zoho ManageEngine ADAudit Plus 7.1.1 allows an attacker to bypass audit detection by creating or renaming user accounts with a "$" symbol suffix. **CVE ID : CVE-2023-32783**	N/A	O-MIC-WIND-220823/4823
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from 4.0.0 through 4.0.2, from 3.1.0 through 3.1.27. **CVE ID : CVE-2023-4136**	N/A	O-MIC-WIND-220823/4824
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-MIC-WIND-220823/4825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20561**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29303**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4826
Insufficient Verification of Data Authenticity	02-Aug-2023	5.5	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached	https://my.f5.com/manage/s/article/K000132563	O-MIC-WIND-220823/4827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-36858**		
N/A	08-Aug-2023	5.5	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD ?Prof may allow an authenticated user to send an arbitrary buffer potentially resulting in a Windows crash leading to denial of service. **CVE ID : CVE-2023-20556**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-7003	O-MIC-WIND-220823/4828
Out-of-bounds Read	09-Aug-2023	5.5	Adobe Dimension version 3.4.9 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-2023-38213**	https://helpx.adobe.com/security/products/dimension/apsb23-44.html	O-MIC-WIND-220823/4829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38229**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4830
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-38235**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38236**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4832
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4833

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-2023-38237**		
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38238**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4834
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38239**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38240**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4836
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38232**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38242**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4838
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-38243**		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38244**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4840
Exposure of Sensitive Information to an	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	https://helpx.adobe.com/security/produc	O-MIC-WIND-220823/4841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page. **CVE ID : CVE-2023-38245**	ts/acrobat/apsb23-30.html	
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38247		
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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-2023-38248**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4843
Use After Free	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38230**		
N/A	01-Aug-2023	5.5	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 102.14, Firefox ESR < 115.1, Thunderbird < 102.14, and Thunderbird < 115.1. **CVE ID : CVE-2023-4054**	https://www.mozilla.org/security/advisories/mfsa2023-30/, https://www.mozilla.org/security/advisories/mfsa2023-31/, https://www.mozilla.org/security/advisories/mfsa2023-29/, https://www.mozilla.org/security/advisories/mfsa2023-33/	O-MIC-WIND-220823/4845
Out-of-bounds Read	10-Aug-2023	5.5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-38241**		
Untrusted Search Path	10-Aug-2023	4.7	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-29299**	https://helpx.adobe.com/security/products/acrobat/apsb23-30.html	O-MIC-WIND-220823/4847
Product: windows_10					
Affected Version(s): * Up to (excluding) 10.0.10240.20107					
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/4849
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/4850
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/4851
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/4852
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/4853
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/4854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36907		
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/4855
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/4856
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/4857
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/4858
Product: windows_10_1507					
Affected Version(s): -					
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/4859
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/4860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-38184**		
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/4861
Affected Version(s): * Up to (excluding) 10.0.10240.20107					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/4862
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/4863
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/4864
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/4865
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35359	bility/CVE-2023-35359	
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/4867
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/4868
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/4869
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/4870
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/4871
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/4872
N/A	08-Aug-2023	5.5	Windows Group Policy Security	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/4873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	guide/vulnerability/CVE-2023-36889	
Product: windows_10_1607					
Affected Version(s): -					
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/4874
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/4875
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/4876
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/4877
Affected Version(s): * Up to (excluding) 10.0.14393.6167					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/4878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/4879
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/4880
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/4881
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/4882
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/4883
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/4884
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/4885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35359	guide/vulnerability/CVE-2023-35359	
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/4886
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/4887
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/4888
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/4889
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/4890
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36906	bility/CVE-2023-36906	
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/4892
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/4893
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/4894
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/4895
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/4896
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/4898
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/4899
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/4900
Product: windows_10_1809					
Affected Version(s): -					
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/4901
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/4902
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38184		
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/4904
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/4905
Affected Version(s): * Up to (excluding) 10.0.17763.4737					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/4906
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/4907
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/4908
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/4909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/4910
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/4911
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/4912
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/4913
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/4914
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/4915
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35386	bility/CVE-2023-35386	
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/4917
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/4918
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38154**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38154	O-MIC-WIND-220823/4919
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/4920
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/4921
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36906	bility/CVE-2023-36906	
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/4923
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/4924
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/4925
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/4926
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/4927
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/4928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35377	guide/vulnerability/CVE-2023-35377	
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/4929
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/4930
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/4931
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/4932
Product: windows_10_21h2					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Windows Mobile Device Management Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38186	O-MIC-WIND-220823/4933
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36899	bility/CVE-2023-36899	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/4935
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/4936
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/4937
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/4938
Affected Version(s): * Up to (excluding) 10.0.19044.3324					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/4939
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36903	bility/CVE-2023-36903	
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/4941
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/4942
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/4943
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/4944
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/4945
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/4946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/4947
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/4948
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/4949
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/4950
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/4951
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/4952
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-36905**	bility/CVE-2023-36905	
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/4954
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/4955
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/4956
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/4957
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/4958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/4959
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/4960
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/4961
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/4962
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/4963
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/4964
Affected Version(s): 10.0.19044.3324					
N/A	08-Aug-2023	5.5	Windows Smart Card Resource Management Server	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36914**	bility/CVE-2023-36914	
Product: windows_10_22h2					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Windows Mobile Device Management Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38186	O-MIC-WIND-220823/4966
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/4967
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/4968
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/4969
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/4970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/4971
Affected Version(s): * Up to (excluding) 10.0.19045.3324					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/4972
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/4973
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/4974
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/4975
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/4976
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/4977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	guide/vulnerability/CVE-2023-35387	
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/4978
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/4979
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/4980
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/4981
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/4982
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/4983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36900		
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/4984
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/4985
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/4986
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/4987
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/4988
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36912	bility/CVE-2023-36912	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/4990
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/4991
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/4992
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/4993
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/4994
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/4995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36908	bility/CVE-2023-36908	
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/4996
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/4997
Affected Version(s): 10.0.19045.3324					
N/A	08-Aug-2023	5.5	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36914**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36914	O-MIC-WIND-220823/4998
Product: windows_11_21h2					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Windows Mobile Device Management Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38186	O-MIC-WIND-220823/4999
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5000
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38172	bility/CVE-2023-38172	
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5002
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5003
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5004
Affected Version(s): * Up to (excluding) 10.0.22000.2295					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5005
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5006
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36910	bility/CVE-2023-36910	
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5008
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5009
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5010
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5011
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5012
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/5014
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5015
N/A	08-Aug-2023	7.8	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability **CVE ID : CVE-2023-36898**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36898	O-MIC-WIND-220823/5016
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5017
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/5018
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/5020
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5021
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5022
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5023
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/5024
Concurrent Execution using Shared Resource with Improper	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/5025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')					
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5026
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5027
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5028
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5029
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5030
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.0.22000.2295					
N/A	08-Aug-2023	5.5	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36914**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36914	O-MIC-WIND-220823/5032
Product: windows_11_22h2					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Windows Mobile Device Management Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38186	O-MIC-WIND-220823/5033
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5034
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5035
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5036
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/5037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36873	guide/vulnerability/CVE-2023-36873	
Affected Version(s): * Up to (excluding) 10.0.22621.2134					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5038
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5039
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5040
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5041
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5042
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35387		
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5044
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5045
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5046
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/5047
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5048
N/A	08-Aug-2023	7.8	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability **CVE ID : CVE-2023-36898**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36898	O-MIC-WIND-220823/5049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5050
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/5051
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5052
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/5053
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5054
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36907		
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5056
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/5057
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/5058
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5059
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5060
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35384	bility/CVE-2023-35384	
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5062
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5063
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5064
Affected Version(s): 10.0.22621.2134					
N/A	08-Aug-2023	5.5	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36914**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36914	O-MIC-WIND-220823/5065
Product: windows_server_2008					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5066
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-36910**	bility/CVE-2023-36910	
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5068
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5069
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5070
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5071
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5072
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bility/CVE-2023-35380	
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5074
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5075
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5076
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5077
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5078
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36913	bility/CVE-2023-36913	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5080
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5081
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5082
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5083
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5084
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5086
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5087
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5088
Affected Version(s): r2					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5089
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5090
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5091
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/5092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-36911**	guide/vulnerability/CVE-2023-36911	
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5093
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5094
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5095
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5096
N/A	08-Aug-2023	7.8	Reliability Analysis Metrics Calculation Engine (RACEng) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35379**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35379	O-MIC-WIND-220823/5097
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35380	bility/CVE-2023-35380	
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5099
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5100
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5101
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5102
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5103
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36913	bility/CVE-2023-36913	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5105
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5106
N/A	08-Aug-2023	7.1	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36876	O-MIC-WIND-220823/5107
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5108
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5109
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35384	bility/CVE-2023-35384	
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5111
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5112
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5113
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5114
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5115
Product: windows_server_2012					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5117
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5118
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5119
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5120
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5121
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5122
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/5123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36899	guide/vulnerability/CVE-2023-36899	
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5124
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5125
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5126
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5127
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5128
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36907		
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5130
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/5131
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5132
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5133
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5134
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5136
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5137
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5138
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5139
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5140
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5141
Affected Version(s): r2					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-35385**	bility/CVE-2023-35385	
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5143
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5144
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5145
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5146
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5147
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36882		
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5149
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5150
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5151
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5152
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5153
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5154
N/A	08-Aug-2023	7.5	Windows Cryptographic	https://msrc.microsoft.com	O-MIC-WIND-220823/5155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	/update-guide/vulnerability/CVE-2023-36906	
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5156
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5157
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/5158
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5159
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5161
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5162
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5163
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5164
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5165
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5166
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bility/CVE-2023-36873	
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5168
Product: windows_server_2016					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5169
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5170
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5171
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5172
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35381	bility/CVE-2023-35381	
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5174
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5175
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5176
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5177
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5178
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5179
N/A	08-Aug-2023	7.8	Windows Common Log File System	https://msrc.microsoft.com	O-MIC-WIND-220823/5180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	/update-guide/vulnerability/CVE-2023-36900	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5181
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/5182
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5183
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5184
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-36913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36913	O-MIC-WIND-220823/5186
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5187
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5188
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5189
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5190
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5191
N/A	08-Aug-2023	6.5	Windows Hyper-V Information	https://msrc.microsoft.com	O-MIC-WIND-220823/5192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-36908**	/update-guide/vulnerability/CVE-2023-36908	
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5193
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5194
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5195
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5196
Product: windows_server_2019					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-35385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385	O-MIC-WIND-220823/5197
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36903	bility/CVE-2023-36903	
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5199
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5200
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5201
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5202
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5203
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5205
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5206
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/5207
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5208
N/A	08-Aug-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36900	O-MIC-WIND-220823/5209
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/5210
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38154	bility/CVE-2023-38154	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5212
N/A	08-Aug-2023	7.5	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability **CVE ID : CVE-2023-36905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36905	O-MIC-WIND-220823/5213
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5214
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5215
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5216
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36913	bility/CVE-2023-36913	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5218
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5219
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/5220
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5221
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35377	O-MIC-WIND-220823/5222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5223
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5224
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5225
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5226
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5227
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5228
Product: windows_server_2022					
Affected Version(s): -					
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote	https://msrc.microsoft.com	O-MIC-WIND-220823/5229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-35385**	/update-guide/vulnerability/CVE-2023-35385	
N/A	08-Aug-2023	9.8	Windows System Assessment Tool Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36903	O-MIC-WIND-220823/5230
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910	O-MIC-WIND-220823/5231
N/A	08-Aug-2023	9.8	Microsoft Message Queuing Remote Code Execution Vulnerability **CVE ID : CVE-2023-36911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911	O-MIC-WIND-220823/5232
N/A	08-Aug-2023	9.8	Windows Mobile Device Management Elevation of Privilege Vulnerability **CVE ID : CVE-2023-38186**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38186	O-MIC-WIND-220823/5233
N/A	08-Aug-2023	8.8	Windows Fax Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-35381**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35381	O-MIC-WIND-220823/5234
N/A	08-Aug-2023	8.8	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35387	O-MIC-WIND-220823/5235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35387		
N/A	08-Aug-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-36882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36882	O-MIC-WIND-220823/5236
N/A	08-Aug-2023	8.8	ASP.NET Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36899	O-MIC-WIND-220823/5237
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35359**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35359	O-MIC-WIND-220823/5238
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35380**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35380	O-MIC-WIND-220823/5239
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35382	O-MIC-WIND-220823/5240
N/A	08-Aug-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35386**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35386	O-MIC-WIND-220823/5241
N/A	08-Aug-2023	7.8	Windows Common Log File System	https://msrc.microsoft.com	O-MIC-WIND-220823/5242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36900**	/update-guide/vulnerability/CVE-2023-36900	
N/A	08-Aug-2023	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-36904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36904	O-MIC-WIND-220823/5243
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2023-35383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35383	O-MIC-WIND-220823/5244
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36906	O-MIC-WIND-220823/5245
N/A	08-Aug-2023	7.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2023-36907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36907	O-MIC-WIND-220823/5246
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36912	O-MIC-WIND-220823/5247
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/5248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-36913**	guide/vulnerability/CVE-2023-36913	
N/A	08-Aug-2023	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38172**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38172	O-MIC-WIND-220823/5249
N/A	08-Aug-2023	7.5	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-38184**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38184	O-MIC-WIND-220823/5250
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Aug-2023	7	Windows Projected File System Elevation of Privilege Vulnerability **CVE ID : CVE-2023-35378**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35378	O-MIC-WIND-220823/5251
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35376**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35376	O-MIC-WIND-220823/5252
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-35377**	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-220823/5253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bility/CVE-2023-35377	
N/A	08-Aug-2023	6.5	Windows HTML Platforms Security Feature Bypass Vulnerability **CVE ID : CVE-2023-35384**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35384	O-MIC-WIND-220823/5254
N/A	08-Aug-2023	6.5	Windows Hyper-V Information Disclosure Vulnerability **CVE ID : CVE-2023-36908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36908	O-MIC-WIND-220823/5255
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-36909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36909	O-MIC-WIND-220823/5256
N/A	08-Aug-2023	6.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2023-38254**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38254	O-MIC-WIND-220823/5257
N/A	08-Aug-2023	5.9	.NET Framework Spoofing Vulnerability **CVE ID : CVE-2023-36873**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36873	O-MIC-WIND-220823/5258
N/A	08-Aug-2023	5.5	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36889**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36889	O-MIC-WIND-220823/5259
N/A	08-Aug-2023	5.5	Windows Smart Card Resource Management Server	https://msrc.microsoft.com/update-	O-MIC-WIND-220823/5260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability **CVE ID : CVE-2023-36914**	guide/vulnerability/CVE-2023-36914	
Vendor: Mitsubishielectric					
Product: c80_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-C80_-220823/5261
Product: e70_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-E70_-220823/5262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: e80_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-E80_-220823/5263
Product: gs21_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					
Use of Insufficiently Random Values	04-Aug-2023	9.1	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-006_en.pdf	O-MIT-GS21-220823/5264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GT21 model versions 01.49.000 and prior and GOT SIMPLE Series GS21 model versions 01.49.000 and prior allows a remote unauthenticated attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it. **CVE ID : CVE-2023-3373**		
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	O-MIT-GS21-220823/5265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gs25_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-GS25-220823/5266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT	lity/pdf/2023-008_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt21_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					
Use of Insufficiently Random Values	04-Aug-2023	9.1	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT21 model versions 01.49.000 and prior and GOT SIMPLE Series GS21 model versions 01.49.000 and prior allows a remote unauthenticated attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it. **CVE ID : CVE-2023-3373**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-006_en.pdf	O-MIT-GT21-220823/5267
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-GT21-220823/5268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT	lity/pdf/2023-008_en.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt23_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	O-MIT-GT23-220823/5269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt25_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	O-MIT-GT25-220823/5270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: gt27_firmware					
Affected Version(s): * Up to (excluding) 01.50.000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	04-Aug-2023	7.5	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-008_en.pdf	O-MIT-GT27-220823/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled. **CVE ID : CVE-2023-0525**		
Product: m70v_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M70V-220823/5272
Product: m720vs_15-type_firmware					
Affected Version(s): -					
Buffer Copy without Checking	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	https://www.mitsubishielectric.com/en/psirt/vulnerabi	O-MIT-M720-220823/5273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	lity/pdf/2023-007_en.pdf	
Product: m720vs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M720-220823/5274
Product: m720vw_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M720-220823/5275
Product: m730vs_15-type_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M730-220823/5276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m730vs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M730-220823/5277
Product: m730vw_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M730-220823/5278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m750vs_15-type_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M750-220823/5279
Product: m750vs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M750-220823/5280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m750vw_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M750-220823/5281
Product: m800s_firmware					
Affected Version(s): -					
Buffer Copy	03-Aug-2023	9.8	Buffer Copy without Checking Size of	https://www.mitsubishielec	O-MIT-M800-220823/5282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	tric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	
Product: m800vs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M800-220823/5283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: m800vw_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M800-220823/5284
Product: m800w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M800-220823/5285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m80vw_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M80V-220823/5286
Product: m80v_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M80V-220823/5287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Product: m80w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M80W-220823/5288
Product: m80_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	03-Aug-2023	9.8	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-007_en.pdf	O-MIT-M80_-220823/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery. **CVE ID : CVE-2023-3346**		
Vendor: Netgear					
Product: dc112a_firmware					
Affected Version(s): 1.0.0.64					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi. **CVE ID : CVE-2023-38925**	https://www.netgear.com/about/security/	O-NET-DC11-220823/5290
Product: dg834gv5_firmware					
Affected Version(s): 1.6.01.34					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DG834Gv5 1.6.01.34 was discovered to contain multiple buffer overflows via the wla_ssid and wla_temp_ssid parameters at bsw_ssid.cgi.	https://www.netgear.com/about/security/	O-NET-DG83-220823/5291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38591		
Product: dgn3500_firmware					
Affected Version(s): 1.1.00.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	6.5	Netgear DGN3500 1.1.00.37 was discovered to contain a buffer overflow via the http_password parameter at setup.cgi. **CVE ID : CVE-2023-38924**	https://www.netgear.com/about/security/	O-NET-DGN3-220823/5292
Product: ex6200_firmware					
Affected Version(s): 1.0.3.94					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi. **CVE ID : CVE-2023-38925**	https://www.netgear.com/about/security/	O-NET-EX62-220823/5293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set. **CVE ID : CVE-2023-38926**	https://www.netgear.com/about/security/	O-NET-EX62-220823/5294
Product: jwnr2000v2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.0.11					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**	https://www.netgear.com/about/security/	O-NET-JWNR-220823/5295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function. **CVE ID : CVE-2023-39550**	https://www.netgear.com/about/security/	O-NET-JWNR-220823/5296
Product: r6300v2_firmware					
Affected Version(s): 1.0.4.8					
Buffer Copy without Checking Size of Input ('Classic	07-Aug-2023	8.8	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd	https://www.netgear.com/about/security/	O-NET-R630-220823/5297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			parameter in password.cgi. **CVE ID : CVE-2023-38925**		
Product: r6900p_firmware					
Affected Version(s): 1.3.3.154					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear R6900P v1.3.3.154 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at ia_ap_setting.cgi. **CVE ID : CVE-2023-38412**	https://www.netgear.com/about/security/	O-NET-R690-220823/5298
Product: r7100lg_firmware					
Affected Version(s): 1.0.0.78					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Aug-2023	9.8	Netgear R7100LG 1.0.0.78 was discovered to contain a command injection vulnerability via the password parameter at usb_remote_invite.cgi. **CVE ID : CVE-2023-38928**	https://www.netgear.com/about/security/	O-NET-R710-220823/5299
Product: wag302v2_firmware					
Affected Version(s): 5.1.19					
Improper Neutralization of Special Elements used in a Command ('Comman	07-Aug-2023	8.8	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler	https://www.netgear.com/about/security/	O-NET-WAG3-220823/5300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			function via the firmwareRestore and firmwareServerip parameters. **CVE ID : CVE-2023-38921**		
Product: wg302v2_firmware					
Affected Version(s): 5.2.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Aug-2023	8.8	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler function via the firmwareRestore and firmwareServerip parameters. **CVE ID : CVE-2023-38921**	https://www.netgear.com/about/security/	O-NET-WG30-220823/5301
Product: xavn2001v2_firmware					
Affected Version(s): 0.4.0.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**	https://www.netgear.com/about/security/	O-NET-XAVN-220823/5302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function. **CVE ID : CVE-2023-39550**	https://www.netgear.com/about/security/	O-NET-XAVN-220823/5303
Product: xr300_firmware					
Affected Version(s): 1.0.3.78					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear XR300 v1.0.3.78 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at genie_ap_wifi_change.cgi. **CVE ID : CVE-2023-36499**	https://www.netgear.com/about/security/	O-NET-XR30-220823/5304
Product: xwn5001_firmware					
Affected Version(s): 0.4.1.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and	https://www.netgear.com/about/security/	O-NET-XWN5-220823/5305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			http_username parameters in the update_auth function. **CVE ID : CVE-2023-38922**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-2023	8.8	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function. **CVE ID : CVE-2023-39550**	https://www.netgear.com/about/security/	O-NET-XWN5-220823/5306
Vendor: Omron					
Product: cj1w-eip21_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ1W-220823/5307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu64-eip_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2H-220823/5308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu65-eip_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in	https://www.ia.omron.com/product/vulnerability/OMSR	O-OMR-CJ2H-220823/5309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**	-2023-006_en.pdf	
Product: cj2h-cpu66-eip_firmware					
Affected Version(s): * Up to (including) 3.04					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2H-220823/5310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu67-eip_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2H-220823/5311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2h-cpu68-eip_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2H-220823/5312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu31_firmware					
Affected Version(s): * Up to (including) 2.18					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2M-220823/5313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu32_firmware					
Affected Version(s): * Up to (including) 2.18					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2M-220823/5314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu33_firmware					
Affected Version(s): * Up to (including) 2.18					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2M-220823/5315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu34_firmware					
Affected Version(s): * Up to (including) 2.18					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2M-220823/5316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cj2m-cpu35_firmware					
Affected Version(s): * Up to (including) 2.18					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CJ2M-220823/5317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Product: cs1w-eip21_firmware					
Affected Version(s): * Up to (including) 3.04					
N/A	03-Aug-2023	7.5	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and	https://www.ia.omron.com/product/vulnerability/OMSR-2023-006_en.pdf	O-OMR-CS1W-220823/5318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier. **CVE ID : CVE-2023-38744**		
Vendor: openwrt					
Product: openwrt					
Affected Version(s): 19.07.0					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-OPE-OPEN-220823/5319
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2023	O-OPE-OPEN-220823/5320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**		
Affected Version(s): 21.02.0					
Out-of-bounds Write	07-Aug-2023	4.4	In nvram, 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. Patch ID: ALPS07740194; Issue ID: ALPS07740194. **CVE ID : CVE-2023-20790**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-OPE-OPEN-220823/5321
Out-of-bounds Write	07-Aug-2023	4.4	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790. **CVE ID : CVE-2023-20796**	https://corp.mediatek.com/product-security-bulletin/August-2023	O-OPE-OPEN-220823/5322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: oppo					
Product: coloros					
Affected Version(s): 12.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Aug-2023	9.8	There is a command injection problem in the old version of the mobile phone backup app. **CVE ID : CVE-2023-26310**	https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-1684402464721477632	O-OPP-COLO-220823/5323
Vendor: Phoenixcontact					
Product: cloud_client_1101t-tx_firmware					
Affected Version(s): * Up to (excluding) 2.06.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-CLOU-220823/5324
Improper Restriction of Recursive Entity	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to	N/A	O-PHO-CLOU-220823/5325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
References in DTDs ('XML Entity Expansion')			2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g_att_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_C-220823/5326
Improper Restriction of Recursive Entity References in DTDs	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT	N/A	O-PHO-TC_C-220823/5327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('XML Entity Expansion')			1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_C-220823/5328
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an	N/A	O-PHO-TC_C-220823/5329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Expansion')			authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_cloud_client_1002-4g_vzw_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_C-220823/5330
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with	N/A	O-PHO-TC_C-220823/5331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin privileges could upload a crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_router_3002t-4g_att_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_R-220823/5332
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a	N/A	O-PHO-TC_R-220823/5333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted XML file which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_router_3002t-4g_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_R-220823/5334
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file	N/A	O-PHO-TC_R-220823/5335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which causes a denial-of-service. **CVE ID : CVE-2023-3569**		
Product: tc_router_3002t-4g_vzw_firmware					
Affected Version(s): * Up to (excluding) 2.07.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2023	9.6	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser. **CVE ID : CVE-2023-3526**	N/A	O-PHO-TC_R-220823/5336
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	08-Aug-2023	4.9	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service.	N/A	O-PHO-TC_R-220823/5337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3569		
Product: wp_6070-wvps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	O-PHO-WP_6-220823/5338
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	O-PHO-WP_6-220823/5339
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain	N/A	O-PHO-WP_6-220823/5340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			full access to the device. **CVE ID : CVE-2023-3571**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	O-PHO-WP_6-220823/5341
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	O-PHO-WP_6-220823/5342
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated	N/A	O-PHO-WP_6-220823/5343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5344
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service	N/A	O-PHO-WP_6-220823/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication of the affected device(s). **CVE ID : CVE-2023-37857**		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	O-PHO-WP_6-220823/5346
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	O-PHO-WP_6-220823/5347
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use	N/A	O-PHO-WP_6-220823/5348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**		
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	O-PHO-WP_6-220823/5349
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	O-PHO-WP_6-220823/5350
Externally Controlled	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx	N/A	O-PHO-WP_6-220823/5351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reference to a Resource in Another Sphere			series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**		
Product: wp_6101-wxps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	O-PHO-WP_6-220823/5352
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to	N/A	O-PHO-WP_6-220823/5353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			gain full access to the device. **CVE ID : CVE-2023-3570**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	O-PHO-WP_6-220823/5354
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	O-PHO-WP_6-220823/5355
Improper Neutralization of Special Elements used in an OS Command	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with	N/A	O-PHO-WP_6-220823/5356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**		
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	O-PHO-WP_6-220823/5357
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5358
Use of Hard-	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in	N/A	O-PHO-WP_6-220823/5359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	O-PHO-WP_6-220823/5360
Improper Neutralization of Special Elements used in an OS	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write	N/A	O-PHO-WP_6-220823/5361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**		
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	O-PHO-WP_6-220823/5362
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	O-PHO-WP_6-220823/5363
Externally Controlled Reference	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in	N/A	O-PHO-WP_6-220823/5364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Resource in Another Sphere			versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	O-PHO-WP_6-220823/5365
Product: wp_6121-wxps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to	N/A	O-PHO-WP_6-220823/5366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	O-PHO-WP_6-220823/5367
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	O-PHO-WP_6-220823/5368
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to	N/A	O-PHO-WP_6-220823/5369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	O-PHO-WP_6-220823/5370
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	O-PHO-WP_6-220823/5371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5372
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	O-PHO-WP_6-220823/5373
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges	N/A	O-PHO-WP_6-220823/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	O-PHO-WP_6-220823/5375
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	O-PHO-WP_6-220823/5376
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with	N/A	O-PHO-WP_6-220823/5377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	O-PHO-WP_6-220823/5378
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser .	N/A	O-PHO-WP_6-220823/5379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37856		
Product: wp_6156-whps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	O-PHO-WP_6-220823/5380
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	O-PHO-WP_6-220823/5381
Improper Neutralization of Special Elements used in an OS Command	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST	N/A	O-PHO-WP_6-220823/5382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	O-PHO-WP_6-220823/5383
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	O-PHO-WP_6-220823/5384
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to	N/A	O-PHO-WP_6-220823/5385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5386
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be	N/A	O-PHO-WP_6-220823/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**		
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	O-PHO-WP_6-220823/5388
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	O-PHO-WP_6-220823/5389
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with	N/A	O-PHO-WP_6-220823/5390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**		
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	O-PHO-WP_6-220823/5391
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	O-PHO-WP_6-220823/5392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	O-PHO-WP_6-220823/5393
Product: wp_6185-whps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**	N/A	O-PHO-WP_6-220823/5394
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a	N/A	O-PHO-WP_6-220823/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	O-PHO-WP_6-220823/5396
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**	N/A	O-PHO-WP_6-220823/5397
Improper Neutralization of Special Elements used in an	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated	N/A	O-PHO-WP_6-220823/5398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**		
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service. **CVE ID : CVE-2023-37862**	N/A	O-PHO-WP_6-220823/5399
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	O-PHO-WP_6-220823/5401
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**	N/A	O-PHO-WP_6-220823/5402
Improper Neutralization of Special	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to	N/A	O-PHO-WP_6-220823/5403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**		
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	O-PHO-WP_6-220823/5404
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**	N/A	O-PHO-WP_6-220823/5405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	O-PHO-WP_6-220823/5406
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser . **CVE ID : CVE-2023-37856**	N/A	O-PHO-WP_6-220823/5407
Product: wp_6215-whps_firmware					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	9.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use	N/A	O-PHO-WP_6-220823/5408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device. **CVE ID : CVE-2023-3572**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device. **CVE ID : CVE-2023-3570**	N/A	O-PHO-WP_6-220823/5409
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device. **CVE ID : CVE-2023-3571**	N/A	O-PHO-WP_6-220823/5410
Improper Neutralization of Special Elements used in an OS	08-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a	N/A	O-PHO-WP_6-220823/5411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			command injection in a HTTP POST request releated to font configuration operations to gain full access to the device. **CVE ID : CVE-2023-3573**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	8.8	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device. **CVE ID : CVE-2023-37861**	N/A	O-PHO-WP_6-220823/5412
Missing Authorization	09-Aug-2023	8.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service.	N/A	O-PHO-WP_6-220823/5413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37862		
Missing Authorization	09-Aug-2023	7.5	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon. **CVE ID : CVE-2023-37860**	N/A	O-PHO-WP_6-220823/5414
Use of Hard-coded Credentials	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s). **CVE ID : CVE-2023-37857**	N/A	O-PHO-WP_6-220823/5415
Improper Privilege Management	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP	N/A	O-PHO-WP_6-220823/5416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root. **CVE ID : CVE-2023-37859**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37863**	N/A	O-PHO-WP_6-220823/5417
Download of Code Without Integrity Check	09-Aug-2023	7.2	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device. **CVE ID : CVE-2023-37864**	N/A	O-PHO-WP_6-220823/5418
Missing Encryption of Sensitive Data	09-Aug-2023	4.9	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an	N/A	O-PHO-WP_6-220823/5419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password. **CVE ID : CVE-2023-37858**		
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser. **CVE ID : CVE-2023-37855**	N/A	O-PHO-WP_6-220823/5420
Externally Controlled Reference to a Resource in Another Sphere	09-Aug-2023	4.3	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog	N/A	O-PHO-WP_6-220823/5421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the embedded Qt browser . **CVE ID : CVE-2023-37856**		
Vendor: Qualcomm					
Product: 205_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-205_-220823/5422
Product: 215_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-215_-220823/5423
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-315_-220823/5424
Product: 8098_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-8098-220823/5425
Product: 8998_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-8998-220823/5426
Product: apq5053-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ5-220823/5427
Product: apq8009_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5428
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5429
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5430
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5431
Product: apq8017_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-APQ8-220823/5432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5433
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5434
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5435
Product: apq8037_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5437
Product: apq8053-aa_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5438
Product: apq8053-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5439
Product: apq8064au_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5440
Product: apq8096au_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5441
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5442
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-APQ8-220823/5443
Product: aqt1000_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5444
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5445
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/	O-QUA-AQT1-220823/5446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5447
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5448
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5449
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5450
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5452
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AQT1-220823/5453
Product: ar8031_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5454
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5456
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5457
Product: ar8035_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5458
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5459
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5461
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5462
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-AR80-220823/5463
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-C-V2-220823/5464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: csra6620_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5465
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5466
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5467
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5468
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5470
Product: csra6640_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5471
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5472
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5473
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	O-QUA-CSRA-220823/5474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5475
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRA-220823/5476
Product: csrb31024_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRB-220823/5477
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRB-220823/5478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRB-220823/5479
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-CSRB-220823/5480
Product: fastconnect_6200_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5481
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5483
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read/write issues. **CVE ID : CVE-2023-28576**		
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5485
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5486
Time-of-check Time-of-	08-Aug-2023	7	The buffer obtained from kernel APIs such as	https://www.qualcomm.com/company/	O-QUA-FAST-220823/5487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	product-security/bulletins/august-2023-bulletin	
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5488
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FAST-220823/5490
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FLIG-220823/5491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537		
Product: fsm10056_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-FSM1-220823/5492
Product: mdm8207_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM8-220823/5493
Product: mdm9205_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5494
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	O-QUA-MDM9-220823/5495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5496
Product: mdm9206_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5497
Product: mdm9207_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5498
Product: mdm9250_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5499
Product: mdm9607_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5500
Product: mdm9628_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5501
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5502
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-MDM9-220823/5503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5504
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5505
Product: mdm9650_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5506
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MDM9-220823/5507
Product: msm8108_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5508
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5509
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5510
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5511
Product: msm8208_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-MSM8-220823/5512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5513
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5514
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5515
Product: msm8209_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5516
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-MSM8-220823/5517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5518
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5519
Product: msm8608_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5520
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5522
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5523
Product: msm8917_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5524
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5525
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	O-QUA-MSM8-220823/5526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5527
Product: msm8920_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5528
Product: msm8937_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5529
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-MSM8-220823/5530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: msm8940_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5531
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5532
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5533
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-MSM8-220823/5534
Product: pm8937_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-PM89-220823/5535
Product: qam8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5536
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5537
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5538
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QAM8-220823/5539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5540
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5541
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5542
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QAM8-220823/5543
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-QAM8-220823/5544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: qca4004_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5545
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5546
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5547
Product: qca4010_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-	https://www.qualcomm.com/company/product-	O-QUA-QCA4-220823/5548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while the device receives DNS response. **CVE ID : CVE-2023-21625**	security/bulletins/august-2023-bulletin	
Product: qca4020_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5549
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5550
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5551
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5552
Product: qca4024_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5553
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA4-220823/5554
Product: qca6174a_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5555
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5556
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5558
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5559
Product: qca6310_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5560
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5561
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	O-QUA-QCA6-220823/5562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5563
Product: qca6320_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5564
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5565
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5566
Product: qca6335_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5567
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5568
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5569
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5570
Product: qca6390_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5572
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5573
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5574
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5575
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5577
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5578
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5579
Product: qca6391_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5580
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21648	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5582
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5583
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5584
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5585
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5586
Access of Resource	08-Aug-2023	7.8	The cam_get_device_priv	https://www.qualcomm.co	O-QUA-QCA6-220823/5587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	m/company/product-security/bulletins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5588
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5589
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-QCA6-220823/5590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5591
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5592
Product: qca6420_firmware					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	O-QUA-QCA6-220823/5593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5594
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5595
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5596
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5597
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666		
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5599
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5600
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5601
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5602
Product: qca6421_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5603
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5604
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5605
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5606
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5608
Product: qca6426_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5609
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5610
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5611
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5613
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5614
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5615
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5617
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5618
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28576		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5620
Product: qca6430_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5621
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5622
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5623
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21650	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5625
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5626
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5627
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5628
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220823/5629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5630
Product: qca6431_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5631
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5632
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5634
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5635
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5636
Product: qca6436_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5637
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5639
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5640
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5641
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5642
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5644
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5645
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5647
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5648
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5649
Product: qca6564au_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5650
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5651
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5652
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5653
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5654
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	O-QUA-QCA6-220823/5655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5656
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5657
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5658
Product: qca6564a_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5660
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5661
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5662
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5663
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5665
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5666
Product: qca6564_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5667
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5668
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5670
Product: qca6574au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5671
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5672
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5673
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5675
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5676
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5677
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5678
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5680
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5681
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5682
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5683
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. **CVE ID : CVE-2023-21647**	tins/august-2023-bulletin	
Product: qca6574a_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5685
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5686
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5687
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5688
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5690
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5691
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5692
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5693
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5695
Product: qca6574_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5696
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5697
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5698
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5700
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5701
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5702
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5703
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/product-	O-QUA-QCA6-220823/5704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5705
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5706
Product: qca6595au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5707
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5708
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5710
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5711
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5712
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5713
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5715
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5716
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5717
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5718
Product: qca6595_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in automotive during system call. **CVE ID : CVE-2023-21643**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5720
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5721
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5722
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5723
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5725
Product: qca6696_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5726
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5727
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5728
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA6-220823/5729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5730
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5731
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5732
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5733
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5735
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5736
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5737
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5738
Product: qca6698aq_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5739
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA6-220823/5740
Product: qca8081_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5741
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5742
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5744
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5745
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5746
Product: qca8337_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5747
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA8-220823/5748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5749
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5750
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5751
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5752
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA8-220823/5753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA8-220823/5754
Product: qca9367_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5755
Product: qca9377_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5756
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCA9-220823/5757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5758
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5759
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5760
Product: qca9379_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5761
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-QCA9-220823/5762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5763
Product: qca9984_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCA9-220823/5764
Product: qcc5100_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5765
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5767
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5768
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5769
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5770
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCC5-220823/5771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcm2290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM2-220823/5772
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM2-220823/5773
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM2-220823/5774
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM2-220823/5775
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM2-220823/5776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Product: qcm4290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5777
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5778
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5779
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5780
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCM4-220823/5781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: qcm4325_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5782
Product: qcm4490_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM4-220823/5783
Product: qcm6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5784
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5786
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5787
Product: qcm6490_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5788
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5789
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCM6-220823/5790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5791
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCM6-220823/5792
Product: qcn6024_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN6-220823/5793
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN6-220823/5794
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-QCN6-220823/5795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: qcn7606_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	9.8	Memory corruption in QESL while processing payload from external ESL device to firmware. **CVE ID : CVE-2023-28561**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN7-220823/5796
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN7-220823/5797
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN7-220823/5798
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN7-220823/5799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Product: qcn9011_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5800
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5801
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5802
Product: qcn9012_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5803
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	O-QUA-QCN9-220823/5804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5805
Product: qcn9024_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5806
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5807
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5808
Product: qcn9074_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5809
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5810
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5811
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5812
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5814
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCN9-220823/5815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: qcs2290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS2-220823/5816
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS2-220823/5817
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS2-220823/5818
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS2-220823/5819
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCS2-220823/5820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: qcs405_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5821
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5822
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5823
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5825
Product: qcs410_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5826
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5827
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5828
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5830
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5831
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5833
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5834
Product: qcs4290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5836
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5837
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5838
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS4-220823/5839
Product: qcs4490_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QCS4-220823/5840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Product: qcs603_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5841
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5842
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5843
Product: qcs605_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5845
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5846
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5847
Product: qcs610_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5848
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5850
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5851
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5852
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5854
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5855
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: qcs6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5857
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5858
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5859
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5860
Product: qcs6490_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5861
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5862
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5863
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5864
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS6-220823/5865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8155_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS8-220823/5866
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS8-220823/5867
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCS8-220823/5868
Product: qcx315_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCX3-220823/5869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCX3-220823/5870
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QCX3-220823/5871
Product: qm215_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QM21-220823/5872
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QM21-220823/5873
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-QM21-220823/5874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: qrb5165m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5875
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5876
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5877
Product: qrb5165n_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5879
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5880
Product: qrb5165_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5881
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5882
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QRB5-220823/5883
Product: qsm8250_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5884
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5885
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5886
Product: qsm8350_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5887
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QSM8-220823/5889
Product: qts110_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-QTS1-220823/5890
Product: s820a_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-S820-220823/5891
Product: sa4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA41-220823/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5893
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5894
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5895
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5896
Product: sa4155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	O-QUA-SA41-220823/5897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5898
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5899
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5900
Product: sa415m_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5901
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-	O-QUA-SA41-220823/5902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA41-220823/5903
Product: sa515m_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA51-220823/5904
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA51-220823/5905
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA51-220823/5906
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	O-QUA-SA51-220823/5907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Product: sa6145p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5908
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5909
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5910
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5911
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	O-QUA-SA61-220823/5912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5913
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5914
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5915
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5917
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5918
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5919
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5920
Product: sa6150p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA61-220823/5921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling service API with invalid address. **CVE ID : CVE-2023-21627**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5922
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5923
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5924
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5925
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5927
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5928
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5929
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5930
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA61-220823/5931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5932
Product: sa6155p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5933
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5934
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5935
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/product-	O-QUA-SA61-220823/5936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5937
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5938
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5939
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5940
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5942
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5943
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5944
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5945
Product: sa6155_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5946
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5947
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5948
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5949
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA61-220823/5951
Product: sa8145p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5952
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5953
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5954
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5956
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5957
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5958
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5959
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5961
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5962
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5963
Product: sa8150p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5964
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA81-220823/5965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in automotive during system call. **CVE ID : CVE-2023-21643**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5966
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5967
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5968
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5969
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5971
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5972
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5973
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5974
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA81-220823/5975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5976
Product: sa8155p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5977
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5978
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5979
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running	https://www.qualcomm.com/company/product-	O-QUA-SA81-220823/5980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5981
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5982
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5983
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5984
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5986
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5987
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5988
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5989
Product: sa8155_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5990
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5991
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5992
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5993
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5995
Product: sa8195p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5996
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5997
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5998
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/5999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6000
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6001
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6002
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6003
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6005
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6006
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA81-220823/6007
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6008
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA82-220823/6009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6010
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6011
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6012
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6014
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6015
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA82-220823/6016
Product: sa8540p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA85-220823/6017
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SA85-220823/6018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA85-220823/6019
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA85-220823/6020
Product: sa9000p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption due to untrusted pointer dereference in automotive during system call. **CVE ID : CVE-2023-21643**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA90-220823/6021
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA90-220823/6022
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	O-QUA-SA90-220823/6023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SA90-220823/6024
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SC81-220823/6025
Product: sd205_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD20-220823/6026
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD20-220823/6027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD20-220823/6028
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD20-220823/6029
Product: sd210_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD21-220823/6030
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD21-220823/6031
Access of Resource Using Incompatib	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of	https://www.qualcomm.com/company/product-	O-QUA-SD21-220823/6032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	security/bulletins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD21-220823/6033
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD21-220823/6034
Product: sd212_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD21-220823/6035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Product: sd429_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD42-220823/6036
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD42-220823/6037
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD42-220823/6038
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD42-220823/6039
Product: sd439_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD43-220823/6040
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD43-220823/6041
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD43-220823/6042
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD43-220823/6043
Product: sd450_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD45-220823/6044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD45-220823/6045
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD45-220823/6046
Product: sd460_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD46-220823/6047
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD46-220823/6048
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD46-220823/6049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD46-220823/6050
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD46-220823/6051
Product: sd480_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD48-220823/6052
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD48-220823/6053
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	O-QUA-SD48-220823/6054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD48-220823/6055
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD48-220823/6056
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD48-220823/6057
Product: sd625_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6059
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6060
Product: sd626_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6061
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6062
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD62-220823/6063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Product: sd632_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD63-220823/6064
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD63-220823/6065
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD63-220823/6066
Product: sd660_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6067
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-SD66-220823/6068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6069
Product: sd662_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6070
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6071
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6072
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	O-QUA-SD66-220823/6073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6074
Product: sd665_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6075
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6076
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6078
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD66-220823/6079
Product: sd670_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6080
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6081
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD67-220823/6082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6083
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6084
Product: sd675_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6085
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6086
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/	O-QUA-SD67-220823/6087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	product-security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6088
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6089
Product: sd678_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6090
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6092
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6093
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD67-220823/6094
Product: sd680_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD68-220823/6095
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD68-220823/6096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD68-220823/6097
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD68-220823/6098
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD68-220823/6099
Product: sd690_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6100
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	O-QUA-SD69-220823/6101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6102
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6103
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6104
Product: sd695_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6105
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to	https://www.qualcomm.co	O-QUA-SD69-220823/6106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6107
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6108
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6109
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD69-220823/6110
Product: sd710_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD71-220823/6111
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD71-220823/6112
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD71-220823/6113
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD71-220823/6114
Product: sd720g_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD72-220823/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD72-220823/6116
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD72-220823/6117
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD72-220823/6118
Product: sd730_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD73-220823/6119
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-SD73-220823/6120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD73-220823/6121
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD73-220823/6122
Product: sd750g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD75-220823/6123
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD75-220823/6124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD75-220823/6125
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD75-220823/6126
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD75-220823/6127
Product: sd765g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6128
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD76-220823/6129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6130
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6131
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6132
Product: sd765_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6133
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	O-QUA-SD76-220823/6134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6135
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6136
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6137
Product: sd768g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6139
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6140
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6141
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD76-220823/6142
Product: sd778g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD77-220823/6143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD77-220823/6144
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD77-220823/6145
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD77-220823/6146
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD77-220823/6147
Product: sd780g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	O-QUA-SD78-220823/6148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD78-220823/6149
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD78-220823/6150
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD78-220823/6151
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD78-220823/6152
Product: sd7c_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD7C-220823/6153
Product: sd835_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD83-220823/6154
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD83-220823/6155
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD83-220823/6156
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD83-220823/6157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: sd845_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD84-220823/6158
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD84-220823/6159
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD84-220823/6160
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD84-220823/6161
Product: sd850_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6162
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6163
Product: sd855_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6164
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6165
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6167
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6168
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6169
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6170
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6172
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD85-220823/6173
Product: sd865_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6174
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6175
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	O-QUA-SD86-220823/6176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6177
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6178
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6179
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6181
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6182
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6183
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6185
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD86-220823/6186
Product: sd870_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD87-220823/6187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6188
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6189
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6190
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6191
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6193
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6194
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD87-220823/6195
Product: sd888_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6196
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SD88-220823/6197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6198
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6199
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6200
Product: sd888_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6202
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6203
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6204
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD88-220823/6205
Product: sda429w_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SDA4-220823/6206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA4-220823/6207
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA4-220823/6208
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA4-220823/6209
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA4-220823/6210
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA4-220823/6211
Product: sda845_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDA8-220823/6212
Product: sdm429w_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM4-220823/6213
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM4-220823/6214
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM4-220823/6215
Product: sdm630_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SDM6-220823/6216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM6-220823/6217
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM6-220823/6218
Product: sdm845_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDM8-220823/6219
Product: sdx12_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX1-220823/6220
Product: sdx24_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX2-220823/6221
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX2-220823/6222
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX2-220823/6223
Product: sdx50m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6224
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SDX5-220823/6225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6226
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6227
Product: sdx55m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6228
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6229
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	O-QUA-SDX5-220823/6230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6231
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6232
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6233
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6234
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is	https://www.qualcomm.com/company/product-	O-QUA-SDX5-220823/6235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received due to improper input validation. **CVE ID : CVE-2023-21647**	security/bulletins/august-2023-bulletin	
Product: sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6236
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6237
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6238
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6239
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-	O-QUA-SDX5-220823/6240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	security/bulletins/august-2023-bulletin	
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6241
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6242
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX5-220823/6243
Product: sdx57m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SDX5-220823/6244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Product: sdx65_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX6-220823/6245
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX6-220823/6246
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX6-220823/6247
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDX6-220823/6248
Product: sdxr1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6249
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6250
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6251
Product: sdxr2_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6252
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SDXR-220823/6253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6254
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6255
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6256
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6257
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SDXR-220823/6259
Product: sd_455_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_4-220823/6260
Product: sd_636_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6261
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6263
Product: sd_675_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6264
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6265
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6266
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_6-220823/6268
Product: sd_8cx_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6269
Product: sd_8cx_gen2_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6270
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd_8cx_gen3_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6272
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6273
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6274
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6275
Incorrect Type	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type	https://www.qualcomm.com/company/	O-QUA-SD_8-220823/6276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6277
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6278
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6279
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SD_8-220823/6280
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is	https://www.qualcomm.com/company/product-	O-QUA-SD_8-220823/6281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received due to improper input validation. **CVE ID : CVE-2023-21647**	security/bulletins/august-2023-bulletin	
Product: sg4150p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SG41-220823/6282
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SG41-220823/6283
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SG41-220823/6284
Product: sm4125_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM41-220823/6285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM41-220823/6286
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM41-220823/6287
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM41-220823/6288
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM41-220823/6289
Product: sm4350-ac_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	O-QUA-SM43-220823/6290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm4350_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6291
Product: sm4375_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6292
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6293
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6295
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6296
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM43-220823/6297
Product: sm4450_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM44-220823/6298
Product: sm6225-ad_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	O-QUA-SM62-220823/6299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: sm6225_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6300
Product: sm6250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6301
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6302
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6303
Product: sm6250_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6304
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6305
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6306
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM62-220823/6307
Product: sm6375_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM63-220823/6308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Product: sm7250p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM72-220823/6309
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM72-220823/6310
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM72-220823/6311
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM72-220823/6312
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM72-220823/6313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: sm7315_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6314
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6315
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6316
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6317
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-SM73-220823/6318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: sm7325p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6319
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6320
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6321
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM73-220823/6323
Product: sm8350-ac_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM83-220823/6324
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM83-220823/6325
Product: sm8350_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM83-220823/6326
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SM83-220823/6327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Product: sm8450_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM84-220823/6328
Product: sm8475_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SM84-220823/6329
Product: smart_audio_100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SMAR-220823/6330
Product: snapdragon_855\+\/860_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Product: snapdragon_855_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6332
Product: snapdragon_865\+_5g_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6333
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-220823/6334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	tins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6335
Product: snapdragon_865_5g_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-220823/6336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	tins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6337
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Product: snapdragon_870_5g_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6339
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6341
Product: snapdragon_8_gen_1_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6342
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SNAP-220823/6343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	tins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6344
Product: snapdragon_ar2_gen_1_platform_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel	https://www.qualcomm.com/company/product-	O-QUA-SNAP-220823/6345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer in media codec decoding. **CVE ID : CVE-2023-28555**	security/bulletins/august-2023-bulletin	
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6346
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6347
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6348
Product: snapdragon_w5\+_gen_1_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**		
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6350
Product: snapdragon_wear_4100\+_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6351
Product: snapdragon_wear_4100\+_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6352
Product: snapdragon_x12_lte_modem_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6353
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6354
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6355
Product: snapdragon_x55_5g_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6357
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28576		
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6359
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6360
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6361
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6362
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6363
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6364
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6366
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6367
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SNAP-220823/6368
Product: ssg2115p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SSG2-220823/6369
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SSG2-220823/6370
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SSG2-220823/6371
Product: ssg2125p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SSG2-220823/6372
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SSG2-220823/6373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SSG2-220823/6374
Product: sw5100p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6375
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6376
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6377
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SW51-220823/6378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21650	tins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6379
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6380
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6382
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6383
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6384
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is	https://www.qualcomm.com/company/product-	O-QUA-SW51-220823/6385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			received due to improper input validation. **CVE ID : CVE-2023-21647**	security/bulletins/august-2023-bulletin	
Product: sw5100_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6386
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6387
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6388
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6389
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SW51-220823/6390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6391
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6392
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SW51-220823/6393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6394
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6395
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SW51-220823/6396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sxr1120_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR1-220823/6397
Product: sxr1230p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR1-220823/6398
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR1-220823/6399
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR1-220823/6400
Product: sxr2130_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6401
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6402
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6403
Time-of-check Time-of-	08-Aug-2023	7	The buffer obtained from kernel APIs such as	https://www.qualcomm.com/company/	O-QUA-SXR2-220823/6404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	product-security/bulletins/august-2023-bulletin	
Product: sxr2150p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6405
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6406
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-SXR2-220823/6407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6408
Product: sxr2230p_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-SXR2-220823/6409
Product: wcd9306_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6410
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21625		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6412
Product: wcd9326_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6413
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6414
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6415
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6417
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6418
Product: wcd9330_firmware					
Affected Version(s): -					
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6419
Product: wcd9335_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6421
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6422
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6423
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6424
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on stack after use. **CVE ID : CVE-2023-21652**	tins/august-2023-bulletin	
Product: wcd9340_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6426
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6427
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6428
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6429
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	O-QUA-WCD9-220823/6430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Product: wcd9341_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6431
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6432
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6433
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6434
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	O-QUA-WCD9-220823/6435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6436
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6437
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6438
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6440
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6441
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6443
Product: wcd9360_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6444
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6445
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6447
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6448
Product: wcd9370_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6449
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6450
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6452
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6453
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6454
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6456
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6457
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6458
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6460
Product: wcd9371_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6461
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6462
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Product: wcd9375_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6464
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6465
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6466
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6467
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6469
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6470
Product: wcd9380_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6471
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6472
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData	https://www.qualcomm.com/company/product-	O-QUA-WCD9-220823/6473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives data with invalid data length. **CVE ID : CVE-2023-21650**	security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6474
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6475
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6476
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6478
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6479
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6480
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6482
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6483
Product: wcd9385_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCD9-220823/6484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21627	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6485
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6486
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6487
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6488
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6490
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCD9-220823/6491
Product: wcn3610_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6492
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6493
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649		
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6495
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6496
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6497
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6498
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives DNS response. **CVE ID : CVE-2023-21625**	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6500
Product: wcn3615_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6501
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6502
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6504
Product: wcn3620_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6505
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6506
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6507
Product: wcn3660b_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while	https://www.qualcomm.com/company/product-	O-QUA-WCN3-220823/6508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling service API with invalid address. **CVE ID : CVE-2023-21627**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6509
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6510
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6511
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6512
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6514
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6515
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6517
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6518
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6519
Product: wcn3660_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6520
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6521
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6522
Product: wcn3680b_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6523
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6525
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6526
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6527
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6528
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6530
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6531
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6532
Time-of-check Time-of-use (TOCTOU)	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	tins/august-2023-bulletin	
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6534
Product: wcn3680_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6535
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28537	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6537
Product: wcn3910_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6538
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6539
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6540
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6542
Product: wcn3950_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6543
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6544
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6545
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus	https://www.qualcomm.com/company/	O-QUA-WCN3-220823/6546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clips with modified content. **CVE ID : CVE-2023-22666**	product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6547
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6548
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28577		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6550
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6551
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6552
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6554
Product: wcn3980_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6555
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6556
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6558
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6559
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6560
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6561
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28575		
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6563
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6564
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6565
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6567
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6568
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21647		
Product: wcn3988_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6570
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6571
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6572
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6573
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6575
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6576
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6577
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6579
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6580
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6581
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6583
Product: wcn3990_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6584
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6585
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6587
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6588
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6589
Product: wcn3991_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6591
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6592
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6593
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6594
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6595
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-WCN3-220823/6596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Product: wcn3998_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6597
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6598
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6599
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6600
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in	https://www.qualcomm.com/company/product-	O-QUA-WCN3-220823/6601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6602
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6603
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6604
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6605
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN3-220823/6606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			velocity checks using more than one key. **CVE ID : CVE-2023-21626**	tins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6607
Product: wcn3999_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6608
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6609
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN3-220823/6610
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services	https://www.qualcomm.com/company/	O-QUA-WCN3-220823/6611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	product-security/bulletins/august-2023-bulletin	
Product: wcn6740_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6612
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6613
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6614
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6615
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper	https://www.qualcomm.com/company/	O-QUA-WCN6-220823/6616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	product-security/bulletins/august-2023-bulletin	
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6617
Product: wcn6750_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6618
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6619
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6621
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6622
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6623
Product: wcn6850_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6624
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN6-220823/6625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21649	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6626
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6627
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6628
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6629
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21652		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6631
Product: wcn6851_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6632
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6633
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6634
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN6-220823/6635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21651	tins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6636
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6637
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6638
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6639
Product: wcn6855_firmware					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	O-QUA-WCN6-220823/6640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6641
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6642
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6643
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6645
Product: wcn6856_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6646
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6647
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6648
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21626		
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6650
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6651
Product: wcn685x-1_firmware					
Affected Version(s): -					
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6652
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6653
Product: wcn685x-5_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6654
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN6-220823/6655
Product: wcn7850_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6656
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6657
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6659
Product: wcn7851_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6660
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6661
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6662
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WCN7-220823/6663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. **CVE ID : CVE-2023-21647**	tins/august-2023-bulletin	
Product: wcn785x-1_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6664
Product: wcn785x-5_firmware					
Affected Version(s): -					
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WCN7-220823/6665
Product: wsa8810_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6666
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6668
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6669
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6670
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6671
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6672
Access of Resource Using Incompatible Type	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WSA8-220823/6673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	tins/august-2023-bulletin	
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6674
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6675
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding.	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WSA8-220823/6676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28555	tins/august-2023-bulletin	
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6677
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6678
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6680
Product: wsa8815_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6681
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6682
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6683
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6685
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6686
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6687
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6688
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So	https://www.qualcomm.com/company/product-security/bulle	O-QUA-WSA8-220823/6689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	tins/august-2023-bulletin	
Out-of-bounds Read	08-Aug-2023	7.5	Information disclosure in Network Services due to buffer over-read while the device receives DNS response. **CVE ID : CVE-2023-21625**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6690
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6691
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6692
Use of Hard-	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to	https://www.qualcomm.com/company/	O-QUA-WSA8-220823/6693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	product-security/bulletins/august-2023-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6694
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6695
Product: wsa8830_firmware					
Affected Version(s): -					
Incorrect Type	08-Aug-2023	7.8	Memory corruption in Trusted Execution	https://www.qualcomm.co	O-QUA-WSA8-220823/6696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	m/company/product-security/bulletins/august-2023-bulletin	
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6697
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6698
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6699
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6700
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22666		
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6702
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6703
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address. **CVE ID : CVE-2023-28577**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6705
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6706
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6707
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6709
Product: wsa8832_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6710
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6711
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wsa8835_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory corruption in Trusted Execution Environment while calling service API with invalid address. **CVE ID : CVE-2023-21627**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6713
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in RIL while trying to send apdu packet. **CVE ID : CVE-2023-21648**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6714
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption in WLAN while running doDriverCmd for an unspecific command. **CVE ID : CVE-2023-21649**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6715
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length. **CVE ID : CVE-2023-21650**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6716
Incorrect Type Conversion or Cast	08-Aug-2023	7.8	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE. **CVE ID : CVE-2023-21651**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Aug-2023	7.8	Memory Corruption in Audio while playing amrwbplus clips with modified content. **CVE ID : CVE-2023-22666**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6718
Out-of-bounds Write	08-Aug-2023	7.8	Memory corruption while allocating memory in COmxApeDec module in Audio. **CVE ID : CVE-2023-28537**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6719
Access of Resource Using Incompatible Type ('Type Confusion')	08-Aug-2023	7.8	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it. **CVE ID : CVE-2023-28575**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6720
Use After Free	08-Aug-2023	7.8	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause UAF of the kernel address. **CVE ID : CVE-2023-28577**		
Out-of-bounds Read	08-Aug-2023	7.5	Transient DOS in Audio while remapping channel buffer in media codec decoding. **CVE ID : CVE-2023-28555**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6722
Improper Authentication	08-Aug-2023	7.1	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key. **CVE ID : CVE-2023-21626**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6723
Use of Hard-coded Credentials	08-Aug-2023	7.1	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use. **CVE ID : CVE-2023-21652**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6724
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Aug-2023	7	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g.	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues. **CVE ID : CVE-2023-28576**		
Improper Input Validation	08-Aug-2023	6.5	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation. **CVE ID : CVE-2023-21647**	https://www.qualcomm.com/company/product-security/bulletins/august-2023-bulletin	O-QUA-WSA8-220823/6726
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 9.0					
Use After Free	07-Aug-2023	7.8	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system. **CVE ID : CVE-2023-4147**	https://access.redhat.com/security/cve/CVE-2023-4147, https://www.spinics.net/lists/stable/msg671573.html, https://bugzilla.redhat.com/show_bug.cgi?id=2225239	O-RED-ENTE-220823/6727
Buffer Copy without Checking Size of	01-Aug-2023	5.5	A buffer overflow flaw was found in base/gdevdevn.c:1973 in devn_pcx_write_rle()	https://git.ghostscript.com/?p=ghostpdl.git;a=commitdif	O-RED-ENTE-220823/6728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			in ghostscript. This issue may allow a local attacker to cause a denial of service via outputting a crafted PDF file for a DEVN device with gs. **CVE ID : CVE-2023-38559**	f;h=d81b82c70bc1	
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a possible rearming of the flower_stats_timer from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4133**	https://access.redhat.com/security/cve/CVE-2023-4133	O-RED-ENTE-220823/6729
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/	O-RED-ENTE-220823/6730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate. **CVE ID : CVE-2023-4194**	20230731164237.48365-3-lersek@redhat.com/	
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	O-RED-ENTE-220823/6731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.0					
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**	https://access.redhat.com/security/cve/CVE-2023-0264	O-RED-ENTE-220823/6732
Affected Version(s): 8.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Aug-2023	5.5	A buffer overflow flaw was found in base/gdevdevn.c:1973 in devn_pcx_write_rle() in ghostscript. This issue may allow a local attacker to cause a denial of service via outputting a crafted PDF file for a DEVN device with gs. **CVE ID : CVE-2023-38559**	https://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=d81b82c70bc1	O-RED-ENTE-220823/6733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4132**	https://access.redhat.com/security/cve/CVE-2023-4132	O-RED-ENTE-220823/6734
Use After Free	03-Aug-2023	5.5	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a possible rearming of the flower_stats_timer from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition. **CVE ID : CVE-2023-4133**	https://access.redhat.com/security/cve/CVE-2023-4133	O-RED-ENTE-220823/6735
Incorrect Authorization	07-Aug-2023	5.5	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized	https://lore.kernel.org/all/20230731164237.48365-1-lersek@redhat.com/, https://lore.kernel.org/all/	O-RED-ENTE-220823/6736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate. **CVE ID : CVE-2023-4194**	20230731164237.48365-2-lersek@redhat.com/, https://lore.kernel.org/all/20230731164237.48365-3-lersek@redhat.com/	
Improper Authentication	04-Aug-2023	5	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact	https://access.redhat.com/security/cve/CVE-2023-0264	O-RED-ENTE-220823/6737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability. **CVE ID : CVE-2023-0264**		
Vendor: renault					
Product: zoe_ev_2021_firmware					
Affected Version(s): From (including) 11.10.2021 Up to (including) 16.01.2023					
N/A	03-Aug-2023	4.6	Renault Zoe EV 2021 automotive infotainment system versions 283C35202R to 283C35519R (builds 11.10.2021 to 16.01.2023) allows attackers to crash the infotainment system by sending arbitrary USB data via a USB device. **CVE ID : CVE-2023-39075**	N/A	O-REN-ZOE_-220823/6738
Vendor: Rockwellautomation					
Product: armor_powerflex_firmware					
Affected Version(s): * Up to (including) 1.003					
Incorrect Calculation	08-Aug-2023	7.5	A vulnerability was discovered in the Rockwell Automation Armor PowerFlex device when the product sends communications to the local event log. Threat actors could exploit this vulnerability by sending an influx of	N/A	O-ROC-ARMO-220823/6739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network commands, causing the product to generate an influx of event log traffic at a high rate. If exploited, the product would stop normal operations and self-reset creating a denial-of-service condition. The error code would need to be cleared prior to resuming normal operations. **CVE ID : CVE-2023-2423**		
Vendor: ruijie					
Product: rg-ew1200g_firmware					
Affected Version(s): 1.0\\(1\\)b1p5					
N/A	05-Aug-2023	8.8	A vulnerability was found in Ruijie RG-EW1200G 1.0(1)B1P5. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /api/sys/set_passwd of the component Administrator Password Handler. The manipulation leads to improper access controls. The attack can be launched remotely.	N/A	O-RUI-RG-E-220823/6740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier VDB-236185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4169**		
Vendor: Samsung					
Product: android					
Affected Version(s): 11.0					
Out-of-bounds Write	10-Aug-2023	9.8	Out-of-bounds write vulnerability in parser_hvcC function of libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers. **CVE ID : CVE-2023-30699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6741
N/A	10-Aug-2023	7.8	Improper access control in HDCP trustlet prior to SMR Aug-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30679**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6742
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation vulnerability within initialize function in	https://security.samsungmobile.com/securityUpdate.sm	O-SAM-ANDR-220823/6743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30681**	sb?year=2023&month=08	
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6744
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30687**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6745
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30688**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30689**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6747
N/A	10-Aug-2023	7.8	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023 Release 1 allows local attacker to privilege escalation. **CVE ID : CVE-2023-30691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6748
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in DoOemFactorySendFactoryBypassCommand of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30693**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6749
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30694		
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxGetVerifyAkey in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30696**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6751
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxCfgSetSimlockPayload in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30697**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6752
N/A	10-Aug-2023	5.5	Improper access control vulnerability in SLocationService prior to SMR Aug-2023 Release 1 allows local attacker to update fake location. **CVE ID : CVE-2023-30654**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6753
N/A	10-Aug-2023	5.5	PendingIntent hijacking in WifiGeofenceManager prior to SMR Aug-2023 Release 1 allows local attacker to arbitrary file access.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30701		
N/A	10-Aug-2023	3.3	Improper access control vulnerability in Telecom prior to SMR Aug-2023 Release 1 allows local attakcers to change TTY mode. **CVE ID : CVE-2023-30685**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6755
N/A	10-Aug-2023	3.3	PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in framework prior to SMR Aug-2023 Release 1 allows local attackers to access ContentProvider without proper permission. **CVE ID : CVE-2023-30700**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6756
Affected Version(s): 12.0					
Out-of-bounds Write	10-Aug-2023	9.8	Out-of-bounds write vulnerability in parser_hvcC function of libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers. **CVE ID : CVE-2023-30699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6757
N/A	10-Aug-2023	7.8	Improper access control in HDCP trustlet prior to SMR Aug-2023 Release 1	https://security.samsungmobile.com/securityUpdate.sm	O-SAM-ANDR-220823/6758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30679**	sb?year=2023&month=08	
Improper Privilege Management	10-Aug-2023	7.8	Improper privilege management vulnerability in MMIGroup prior to SMR Aug-2023 Release 1 allows code execution with privilege. **CVE ID : CVE-2023-30680**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6759
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation vulnerability within initialize function in HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30681**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6760
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6761
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR Aug-2023	https://security.samsungmobile.com/securityUpdate.sm	O-SAM-ANDR-220823/6762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30687**	sb?year=2023&month=08	
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30688**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6763
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30689**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6764
N/A	10-Aug-2023	7.8	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023 Release 1 allows local attacker to privilege escalation. **CVE ID : CVE-2023-30691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6765
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in DoOemFactorySendF	https://security.samsungmobile.com/secu	O-SAM-ANDR-220823/6766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actoryBypassCommand of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30693**	rityUpdate.smsb?year=2023&month=08	
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30694**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6767
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxGetVerifyAkey in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30696**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6768
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxCfgSetSimlockPayload in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30697**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Aug-2023	5.5	Improper access control vulnerability in SLocationService prior to SMR Aug-2023 Release 1 allows local attacker to update fake location. **CVE ID : CVE-2023-30654**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6770
N/A	10-Aug-2023	5.5	PendingIntent hijacking in WifiGeofenceManager prior to SMR Aug-2023 Release 1 allows local attacker to arbitrary file access. **CVE ID : CVE-2023-30701**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6771
N/A	10-Aug-2023	3.3	Improper access control vulnerability in Telecom prior to SMR Aug-2023 Release 1 allows local attakcers to change TTY mode. **CVE ID : CVE-2023-30685**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6772
N/A	10-Aug-2023	3.3	PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in framework prior to SMR Aug-2023 Release 1 allows local attackers to access ContentProvider without proper permission.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30700		
Affected Version(s): 13.0					
Out-of-bounds Write	10-Aug-2023	9.8	Out-of-bounds write vulnerability in parser_hvcC function of libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers. **CVE ID : CVE-2023-30699**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6774
N/A	10-Aug-2023	7.8	Improper access control in HDCP trustlet prior to SMR Aug-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-30679**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6775
Improper Privilege Management	10-Aug-2023	7.8	Improper privilege management vulnerability in MMIGroup prior to SMR Aug-2023 Release 1 allows code execution with privilege. **CVE ID : CVE-2023-30680**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6776
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation vulnerability within initialize function in HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows attacker to	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause out-of-bounds write. **CVE ID : CVE-2023-30681**		
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30686**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6778
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30687**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6779
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30688**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6780
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse of libsec-ril prior to SMR Aug-2023	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30689**		
N/A	10-Aug-2023	7.8	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023 Release 1 allows local attacker to privilege escalation. **CVE ID : CVE-2023-30691**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6782
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in DoOemFactorySendFactoryBypassCommand of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30693**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6783
Out-of-bounds Write	10-Aug-2023	7.8	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30694**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6784
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxGetVerifyAkey	https://security.samsungmobile.com/secu	O-SAM-ANDR-220823/6785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30696**	rityUpdate.smsb?year=2023&month=08	
Out-of-bounds Write	10-Aug-2023	7.8	An improper input validation in IpcTxCfgSetSimlockPayload in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write. **CVE ID : CVE-2023-30697**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6786
N/A	10-Aug-2023	5.5	Improper access control vulnerability in SLocationService prior to SMR Aug-2023 Release 1 allows local attacker to update fake location. **CVE ID : CVE-2023-30654**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6787
N/A	10-Aug-2023	5.5	Improper access control vulnerability in TelephonyUI prior to SMR Aug-2023 Release 1 allows local attacker to connect BLE without privilege. **CVE ID : CVE-2023-30698**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6788
N/A	10-Aug-2023	5.5	PendingIntent hijacking in WifiGeofenceManage	https://security.samsungmobile.com/secu	O-SAM-ANDR-220823/6789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r prior to SMR Aug-2023 Release 1 allows local attacker to arbitrary file access. **CVE ID : CVE-2023-30701**	rityUpdate.smsb?year=2023&month=08	
N/A	10-Aug-2023	3.3	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call silenceRinger API without permission. **CVE ID : CVE-2023-30682**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6790
N/A	10-Aug-2023	3.3	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call endCall API without permission. **CVE ID : CVE-2023-30683**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6791
N/A	10-Aug-2023	3.3	Improper access control in Samsung Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call acceptRingingCall API without permission. **CVE ID : CVE-2023-30684**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6792
N/A	10-Aug-2023	3.3	Improper access control vulnerability in Telecom prior to	https://security.samsungmobile.com/secu	O-SAM-ANDR-220823/6793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMR Aug-2023 Release 1 allows local attakcers to change TTY mode. **CVE ID : CVE-2023-30685**	rityUpdate.smsb?year=2023&month=08	
N/A	10-Aug-2023	3.3	PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in framework prior to SMR Aug-2023 Release 1 allows local attackers to access ContentProvider without proper permission. **CVE ID : CVE-2023-30700**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=08	O-SAM-ANDR-220823/6794
Product: galaxy_book2_go_firmware					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	O-SAM-GALA-220823/6795
Product: galaxy_book2_pro_360_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	O-SAM-GALA-220823/6796
Product: galaxy_book_go_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	O-SAM-GALA-220823/6797
Product: galaxy_book_go_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Aug-2023	7.8	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-30702**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=08	O-SAM-GALA-220823/6798
Product: s3nrn4v_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-S3NR-220823/6799
Product: s3nrn82_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-S3NR-220823/6800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**		
Product: s3nsen4_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-S3NS-220823/6801
Product: s3nsn4v_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-S3NS-220823/6802
Product: sen82ab_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	08-Aug-2023	4.3	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB,	https://semiconductor.samsung.com/support/quality-support/prod	O-SAM-SEN8-220823/6803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart. **CVE ID : CVE-2023-36482**	uct-security-updates/	
Vendor: shelly					
Product: pro_4pm_firmware					
Affected Version(s): 0.11.0					
Out-of-bounds Read	02-Aug-2023	5.3	Shelly 4PM Pro four-channel smart switch 0.11.0 allows an attacker to trigger a BLE out of bounds read fault condition that results in a device reload. **CVE ID : CVE-2023-33383**	N/A	O-SHE-PRO_-220823/6804
Vendor: Tenda					
Product: 4g300_firmware					
Affected Version(s): 1.01.42					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda 4G300 v1.01.42 was discovered to contain a stack overflow via the page parameter at /VirtualSer. **CVE ID : CVE-2023-38929**	N/A	O-TEN-4G30-220823/6805
Product: ac10_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6	N/A	O-TEN-AC10-220823/6806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-AC10-220823/6807
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC10-220823/6808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	O-TEN-AC10-220823/6809
Affected Version(s): 16.03.10.13					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203	N/A	O-TEN-AC10-220823/6810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	O-TEN-AC10-220823/6811
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list	N/A	O-TEN-AC10-220823/6812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: ac1206_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	O-TEN-AC12-220823/6813
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the	N/A	O-TEN-AC12-220823/6814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formSetClientState function. **CVE ID : CVE-2023-38933**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	O-TEN-AC12-220823/6815
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC12-220823/6816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	O-TEN-AC12-220823/6817
Product: ac5_firmware					
Affected Version(s): 15.03.06.28					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	O-TEN-AC5_-220823/6818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	O-TEN-AC5_-220823/6819
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-AC5_-220823/6820
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10	N/A	O-TEN-AC5_-220823/6821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC5_-220823/6822
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0	N/A	O-TEN-AC5_-220823/6823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: ac6_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**	N/A	O-TEN-AC6_-220823/6824
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were	N/A	O-TEN-AC6_-220823/6825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC6_-220823/6826
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0	N/A	O-TEN-AC6_-220823/6827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: ac7_firmware					
Affected Version(s): 15.03.06.44					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	O-TEN-AC7_-220823/6828
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack	N/A	O-TEN-AC7_-220823/6829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-AC7_-220823/6830
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC7_-220823/6831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			formSetSpeedWan function. **CVE ID : CVE-2023-38936**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	O-TEN-AC7_-220823/6832
Product: ac8_firmware					
Affected Version(s): 16.03.34.06					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list	N/A	O-TEN-AC8_-220823/6833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**	N/A	O-TEN-AC8_-220823/6834
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**	N/A	O-TEN-AC8_-220823/6835
Product: ac9_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 15.03.06.42_multi					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	O-TEN-AC9_-220823/6836
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-AC9_-220823/6837
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10	N/A	O-TEN-AC9_-220823/6838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function. **CVE ID : CVE-2023-38935**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/formSetSpeedWan/README.md	O-TEN-AC9_-220823/6839
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0	N/A	O-TEN-AC9_-220823/6840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2023-38937**		
Product: f1202_firmware					
Affected Version(s): 1.2.0.9					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**	N/A	O-TEN-F120-220823/6841
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	O-TEN-F120-220823/6842
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9 and FH1202 V1.2.0.9 were	N/A	O-TEN-F120-220823/6843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the mit_ssid parameter in the formWrlsafeset function. **CVE ID : CVE-2023-38939**		
Product: f1203_firmware					
Affected Version(s): 2.0.1.6					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**	N/A	O-TEN-F120-220823/6844
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack	N/A	O-TEN-F120-220823/6845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-F120-220823/6846
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	O-TEN-F120-220823/6847
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23,	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/for	O-TEN-F120-220823/6848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	mSetSpeedWan/README.md	
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**	N/A	O-TEN-F120-220823/6849
Product: fh1202_firmware					
Affected Version(s): 1.2.0.9					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function.	N/A	O-TEN-FH12-220823/6850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38932		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	O-TEN-FH12-220823/6851
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the mit_ssid parameter in the formWrlsafeset function. **CVE ID : CVE-2023-38939**	N/A	O-TEN-FH12-220823/6852
Product: fh1203_firmware					
Affected Version(s): 2.0.1.6					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack	N/A	O-TEN-FH12-220823/6853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the list parameter in the setaccount function. **CVE ID : CVE-2023-38931**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-FH12-220823/6854
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	O-TEN-FH12-220823/6855
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23,	https://github.com/FirmRec/IoT-Vulns/blob/main/tenda/for	O-TEN-FH12-220823/6856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	mSetSpeedWan/README.md	
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**	N/A	O-TEN-FH12-220823/6857
Product: fh1205_firmware					
Affected Version(s): 2.0.0.7\\(775\\)					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the	N/A	O-TEN-FH12-220823/6858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2023-38930**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2023-38933**	N/A	O-TEN-FH12-220823/6859
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function. **CVE ID : CVE-2023-38934**	N/A	O-TEN-FH12-220823/6860
Out-of-bounds Write	07-Aug-2023	9.8	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6	https://github.com/FirmRec/IoT-Vulns/blob/m	O-TEN-FH12-220823/6861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function. **CVE ID : CVE-2023-38936**	ain/tenda/formSetSpeedWan/README.md	
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-38940**	N/A	O-TEN-FH12-220823/6862
Product: pa202_firmware					
Affected Version(s): 1.1.2.5					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in	N/A	O-TEN-PA20-220823/6863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the SafeEmailFilter function. **CVE ID : CVE-2023-38932**		
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im. **CVE ID : CVE-2023-38938**	N/A	O-TEN-PA20-220823/6864
Product: pw201a_firmware					
Affected Version(s): 1.1.2.5					
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function. **CVE ID : CVE-2023-38932**	N/A	O-TEN-PW20-220823/6865
Out-of-bounds Write	07-Aug-2023	9.8	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7Im.	N/A	O-TEN-PW20-220823/6866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38938		
Vendor: totolink					
Product: t10_v2_firmware					
Affected Version(s): 5.9c.5061_b20200511					
Out-of-bounds Write	08-Aug-2023	9.8	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setWiFiWpsConfig in /lib/cste_modules/wps.so. Attackers can send crafted data in an MQTT packet, via the pin parameter, to control the return address and execute code. **CVE ID : CVE-2023-40041**	N/A	O-TOT-T10_-220823/6867
Out-of-bounds Write	08-Aug-2023	9.8	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setStaticDhcpConfig in /lib/cste_modules/lan.so. Attackers can send crafted data in an MQTT packet, via the comment parameter, to control the return address and execute code. **CVE ID : CVE-2023-40042**	N/A	O-TOT-T10_-220823/6868
Vendor: Tp-link					
Product: archer_ax21_firmware					
Affected Version(s): 3_1.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2023	9.8	TP-Link Archer AX21(US)_V3_1.1.4 Build 20230219 and AX21(US)_V3.6_1.1.4 Build 20230219 are vulnerable to Buffer Overflow. **CVE ID : CVE-2023-31710**	N/A	O-TP--ARCH-220823/6869
Affected Version(s): 3.6_1.1.4					
Out-of-bounds Write	01-Aug-2023	9.8	TP-Link Archer AX21(US)_V3_1.1.4 Build 20230219 and AX21(US)_V3.6_1.1.4 Build 20230219 are vulnerable to Buffer Overflow. **CVE ID : CVE-2023-31710**	N/A	O-TP--ARCH-220823/6870