National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 Jan 2024 Vol. 11 No. 01

Table of Content

Vendor	Product	Page Number
Qualcomm	qcn9011	1095
	qcn9012	1098
	qcn9013	1101
	qcn9022	1102
	qcn9024	1104
	qcn9070	1107
	qcn9072	1108
	qcn9074	1109
	qcn9100	1111
	qcn9274	1112
	qcs2290	1113
	qcs410	1115
	qcs4290	1118
	qcs4490	1121
	qcs610	1123
	qcs6125	1127
	qcs6490	1129
	qcs7230	1132
	qcs8155	1135
	qcs8250	1135
	qcs8550	1139
	qdu1000	1142
	qdu1010	1143
	qdu1110	1144
	qdu1210	1145
	qdx1010	1146
	qdx1011	1147
	qet4101	1148
	qfw7114	1148
	qfw7124	1150
	qrb5165m	1152
	qrb5165n	1155

Vendor	Product	Page Number
Qualcomm	qru1032	1158
	qru1052	1159
	qru1062	1160
	qsm8250	1161
	qsm8350	1162
	qsw8573	1164
	qts110	1164
	qualcomm_205_mobile_platform	1164
	qualcomm_215_mobile_platform	1165
	qualcomm_video_collaboration_vc1_platform	1167
	qualcomm_video_collaboration_vc3_platform	1169
	qualcomm_video_collaboration_vc5_platform	1172
	robotics_rb3_platform	1175
	robotics_rb5_platform	1177
	sa4150p	1180
	sa4155p	1184
	sa6145p	1187
	sa6150p	1191
	sa6155	1195
	sa6155p	1197
	sa8145p	1202
	sa8150p	1206
	sa8155	1210
	sa8155p	1212
	sa8195p	1217
	sa8255p	1222
	sa8295p	1225
	sa8540p	1229
	sa9000p	1230
	sc8180x\+sdx55	1230
	sd460	1232
	sd626	1233

Vendor	Product	Page Number
Qualcomm	smart_display_200_platform	1295
	snapdragon_1100_wearable_platform	1295
	snapdragon_1200_wearable_platform	1296
	snapdragon_208_processor	1297
	snapdragon_210_processor	1297
	snapdragon_212_mobile_platform	1298
	snapdragon_425_mobile_platform	1299
	snapdragon_427_mobile_platform	1299
	snapdragon_429_mobile_platform	1300
	snapdragon_430_mobile_platform	1301
	snapdragon_435_mobile_platform	1302
	snapdragon_439_mobile_platform	1303
	snapdragon_450_mobile_platform	1304
	snapdragon_460_mobile_platform	1305
	snapdragon_480\+_5g_mobile_platform	1308
	snapdragon_480_5g_mobile_platform	1311
	snapdragon_4_gen_1_mobile_platform	1315
	snapdragon_4_gen_2_mobile_platform	1319
	snapdragon_625_mobile_platform	1320
	snapdragon_626_mobile_platform	1320
	snapdragon_630_mobile_platform	1321
	snapdragon_632_mobile_platform	1322
	snapdragon_636_mobile_platform	1323
	snapdragon_660_mobile_platform	1324
	snapdragon_662_mobile_platform	1327
	snapdragon_665_mobile_platform	1330
	snapdragon_670_mobile_platform	1333
	snapdragon_675_mobile_platform	1335
	snapdragon_678_mobile_platform	1338
	snapdragon_680_4g_mobile_platform	1340
	snapdragon_685_4g_mobile_platform	1345
	snapdragon_690_5g_mobile_platform	1349

Vendor	Product	Page Number
Qualcomm	snapdragon_695_5g_mobile_platform	1352
	snapdragon_710_mobile_platform	1356
	snapdragon_712_mobile_platform	1358
	snapdragon_720g_mobile_platform	1359
	snapdragon_730g_mobile_platform	1362
	snapdragon_730_mobile_platform	1365
	snapdragon_732g_mobile_platform	1367
	snapdragon_750g_5g_mobile_platform	1370
	snapdragon_765g_5g_mobile_platform	1373
	snapdragon_765_5g_mobile_platform	1377
	snapdragon_768g_5g_mobile_platform	1380
	snapdragon_778g\+_5g_mobile_platform	1384
	snapdragon_778g_5g_mobile_platform	1387
	snapdragon_780g_5g_mobile_platform	1391
	snapdragon_782g_mobile_platform	1394
	snapdragon_7c\+_gen_3_compute	1398
	snapdragon_7c_compute_platform	1401
	snapdragon_7c_gen_2_compute_platform	1403
	snapdragon_808_processor	1405
	snapdragon_810_processor	1406
	snapdragon_820_automotive_platform	1406
	snapdragon_820_mobile_platform	1408
	snapdragon_821_mobile_platform	1409
	snapdragon_835_mobile_pc_platform	1410
	snapdragon_845_mobile_platform	1412
	snapdragon_850_mobile_compute_platform	1413
	snapdragon_855\+\/860_mobile_platform	1415
	snapdragon_855_mobile_platform	1418
	snapdragon_865\+_5g_mobile_platform	1421
	snapdragon_865_5g_mobile_platform	1425
	snapdragon_870_5g_mobile_platform	1428
	snapdragon_888\+_5g_mobile_platform	1432

Vendor	Product	Page Number
Qualcomm	snapdragon_888_5g_mobile_platform	1436
	snapdragon_8cx_compute_platform	1440
	snapdragon_8cx_gen_2_5g_compute_platform	1442
	snapdragon_8cx_gen_3_compute_platform	1444
	snapdragon_8c_compute_platform	1446
	snapdragon_8\+_gen_1_mobile_platform	1448
	snapdragon_8\+_gen_2_mobile_platform	1451
	snapdragon_8_gen_1_mobile_platform	1453
	snapdragon_8_gen_2_mobile_platform	1456
	snapdragon_ar2_gen_1_platform	1459
	snapdragon_auto_4g_modem	1461
	snapdragon_auto_5g_modem-rf	1463
	snapdragon_w5\+_gen_1_wearable_platform	1467
	snapdragon_wear_1300_platform	1472
	snapdragon_wear_2100_platform	1473
	snapdragon_wear_2500_platform	1474
	snapdragon_wear_3100_platform	1475
	snapdragon_wear_4100\+_platform	1476
	snapdragon_x12_lte_modem	1478
	snapdragon_x20_lte_modem	1480
	snapdragon_x24_lte_modem	1481
	snapdragon_x50_5g_modem-rf_system	1483
	snapdragon_x55_5g_modem-rf_system	1486
	snapdragon_x5_lte_modem	1490
	snapdragon_x65_5g_modem-rf_system	1491
	snapdragon_x70_modem-rf_system	1494
	snapdragon_x75_5g_modem-rf_system	1496
	snapdragon_xr1_platform	1498
	snapdragon_xr2\+_gen_1_platform	1499
	snapdragon_xr2_5g_platform	1502
	ssg2115p	1506
	ssg2125p	1508

Vendor	Product	Page Number
Qualcomm	sw5100	1510
	sw5100p	1515
	sxr1120	1519
	sxr1230p	1521
	sxr2130	1523
	sxr2230p	1526
	vision_intelligence_100_platform	1528
	vision_intelligence_200_platform	1529
	vision_intelligence_300_platform	1530
	vision_intelligence_400_platform	1532
	wcd9306	1534
	wcd9326	1535
	wcd9330	1538
	wcd9335	1540
	wcd9340	1544
	wcd9341	1547
	wcd9360	1552
	wcd9370	1554
	wcd9371	1559
	wcd9375	1561
	wcd9380	1566
	wcd9385	1571
	wcd9390	1576
	wcd9395	1578
	wcn3610	1581
	wcn3615	1583
	wcn3620	1585
	wcn3660	1586
	wcn3660b	1587
	wcn3680	1590
	wcn3680b	1591
	wcn3910	1594

Vendor	Product	Page Number
Qualcomm	9206_lte_modem_firmware	1948
	9207_lte_modem_firmware	1949
	apq8017_firmware	1949
	apq8037_firmware	1950
	apq8064au_firmware	1951
	apq8076_firmware	1952
	apq8084_firmware	1952
	apq8092_firmware	1952
	apq8094_firmware	1952
	aqt1000_firmware	1953
	ar8031_firmware	1955
	ar8035_firmware	1957
	ar9380_firmware	1962
	c-v2x_9150_firmware	1962
	csr8811_firmware	1964
	csra6620_firmware	1965
	csra6640_firmware	1968
	csrb31024_firmware	1972
	fastconnect_6200_firmware	1973
	fastconnect_6700_firmware	1978
	fastconnect_6800_firmware	1982
	fastconnect_6900_firmware	1985
	fastconnect_7800_firmware	1990
	flight_rb5_5g_platform_firmware	1994
	fsm10056_firmware	1997
	home_hub_100_platform_firmware	1998
	immersive_home_214_platform_firmware	1998
	immersive_home_216_platform_firmware	1999
	immersive_home_316_platform_firmware	2000
	immersive_home_318_platform_firmware	2001
	immersive_home_3210_platform_firmware	2002
	immersive_home_326_platform_firmware	2003

Vendor	Product	Page Number
Qualcomm	ipq4018_firmware	2004
	ipq4019_firmware	2004
	ipq4028_firmware	2005
	ipq4029_firmware	2005
	ipq5010_firmware	2006
	ipq5028_firmware	2007
	ipq5332_firmware	2008
	ipq6000_firmware	2008
	ipq6005_firmware	2010
	ipq6010_firmware	2010
	ipq6018_firmware	2011
	ipq6028_firmware	2013
	ipq8064_firmware	2014
	ipq8065_firmware	2015
	ipq8068_firmware	2016
	ipq8069_firmware	2016
	ipq8070a_firmware	2017
	ipq8070_firmware	2018
	ipq8071a_firmware	2019
	ipq8072a_firmware	2020
	ipq8074a_firmware	2020
	ipq8074_firmware	2021
	ipq8076a_firmware	2022
	ipq8076_firmware	2023
	ipq8078a_firmware	2024
	ipq8078_firmware	2024
	ipq8173_firmware	2025
	ipq8174_firmware	2026
	ipq9008_firmware	2027
	ipq9554_firmware	2028
	ipq9570_firmware	2029
	ipq9574_firmware	2030

Vendor	Product	Page Number
Qualcomm	mdm8207_firmware	2031
	mdm9225m_firmware	2031
	mdm9225_firmware	2031
	mdm9230_firmware	2032
	mdm9235m_firmware	2032
	mdm9250_firmware	2032
	mdm9330_firmware	2033
	mdm9625m_firmware	2034
	mdm9625_firmware	2034
	mdm9628_firmware	2034
	mdm9630_firmware	2035
	mdm9635m_firmware	2036
	mdm9640_firmware	2036
	mdm9645_firmware	2037
	mdm9650_firmware	2037
	msm8108_firmware	2038
	msm8209_firmware	2039
	msm8608_firmware	2040
	msm8909w_firmware	2040
	msm8996au_firmware	2041
	pm8937_firmware	2042
	pmp8074_firmware	2042
	qam8255p_firmware	2043
	qam8295p_firmware	2047
	qam8650p_firmware	2051
	qam8775p_firmware	2054
	qca0000_firmware	2057
	qca1023_firmware	2058
	qca1062_firmware	2059
	qca1064_firmware	2059
	qca1990_firmware	2060
	qca2062_firmware	2060

Vendor	Product	Page Number
Qualcomm	qca2064_firmware	2061
	qca2065_firmware	2062
	qca2066_firmware	2062
	qca4004_firmware	2063
	qca4024_firmware	2064
	qca4531_firmware	2065
	qca6174a_firmware	2065
	qca6174_firmware	2068
	qca6175a_firmware	2069
	qca6234_firmware	2069
	qca6310_firmware	2069
	qca6320_firmware	2071
	qca6335_firmware	2072
	qca6391_firmware	2073
	qca6420_firmware	2078
	qca6421_firmware	2081
	qca6426_firmware	2084
	qca6428_firmware	2086
	qca6430_firmware	2087
	qca6431_firmware	2090
	qca6436_firmware	2092
	qca6438_firmware	2095
	qca6554a_firmware	2096
	qca6564au_firmware	2097
	qca6564a_firmware	2099
	qca6564_firmware	2101
	qca6574au_firmware	2102
	qca6574a_firmware	2107
	qca6574_firmware	2111
	qca6584au_firmware	2115
	qca6584_firmware	2117
	qca6595au_firmware	2118

Vendor	Product	Page Number
Qualcomm	qca6595_firmware	2122
	qca6678aq_firmware	2127
	qca6696_firmware	2127
	qca6698aq_firmware	2132
	qca6797aq_firmware	2136
	qca7500_firmware	2140
	qca8072_firmware	2140
	qca8075_firmware	2141
	qca8081_firmware	2142
	qca8082_firmware	2147
	qca8084_firmware	2148
	qca8085_firmware	2149
	qca8337_firmware	2150
	qca8386_firmware	2154
	qca9367_firmware	2156
	qca9377_firmware	2156
	qca9379_firmware	2159
	qca9880_firmware	2160
	qca9886_firmware	2160
	qca9888_firmware	2161
	qca9889_firmware	2162
	qca9898_firmware	2163
	qca9980_firmware	2164
	qca9984_firmware	2165
	qca9985_firmware	2166
	qca9986_firmware	2167
	qca9990_firmware	2167
	qca9992_firmware	2168
	qca9994_firmware	2169
	qcc2073_firmware	2170
	qcc2076_firmware	2171
	qcc710_firmware	2171

Vendor	Product	Page Number
Qualcomm	qcf8001_firmware	2173
	qcm2290_firmware	2174
	qcm4290_firmware	2176
	qcm4325_firmware	2178
	qcm4490_firmware	2182
	qcm6125_firmware	2184
	qcm6490_firmware	2186
	qcm8550_firmware	2189
	qcn5021_firmware	2192
	qcn5022_firmware	2193
	qcn5024_firmware	2194
	qcn5052_firmware	2195
	qcn5054_firmware	2196
	qcn5121_firmware	2197
	qcn5122_firmware	2197
	qcn5124_firmware	2199
	qcn5152_firmware	2199
	qcn5154_firmware	2201
	qcn5164_firmware	2202
	qcn6023_firmware	2202
	qcn6024_firmware	2204
	qcn6100_firmware	2207
	qcn6102_firmware	2207
	qcn6112_firmware	2208
	qcn6122_firmware	2209
	qcn6132_firmware	2210
	qcn6224_firmware	2211
	qcn6274_firmware	2213
	qcn7605_firmware	2214
	qcn7606_firmware	2215
	qcn9000_firmware	2216
	qcn9001_firmware	2217

Vendor	Product	Page Number
Qualcomm	qcn9002_firmware	2218
	qcn9003_firmware	2219
	qcn9011_firmware	2220
	qcn9012_firmware	2223
	qcn9013_firmware	2226
	qcn9022_firmware	2227
	qcn9024_firmware	2228
	qcn9070_firmware	2231
	qcn9072_firmware	2232
	qcn9074_firmware	2234
	qcn9100_firmware	2235
	qcn9274_firmware	2236
	qcs2290_firmware	2237
	qcs410_firmware	2239
	qcs4290_firmware	2243
	qcs4490_firmware	2245
	qcs610_firmware	2248
	qcs6125_firmware	2251
	qcs6490_firmware	2253
	qcs7230_firmware	2257
	qcs8155_firmware	2260
	qcs8250_firmware	2260
	qcs8550_firmware	2263
	qdu1000_firmware	2267
	qdu1010_firmware	2268
	qdu1110_firmware	2269
	qdu1210_firmware	2270
	qdx1010_firmware	2271
	qdx1011_firmware	2272
	qet4101_firmware	2273
	qfw7114_firmware	2273
	qfw7124_firmware	2275

Vendor	Product	Page Number
Qualcomm	qrb5165m_firmware	2276
	qrb5165n_firmware	2280
	qru1032_firmware	2283
	qru1052_firmware	2284
	qru1062_firmware	2285
	qsm8250_firmware	2286
	qsm8350_firmware	2287
	qsw8573_firmware	2288
	qts110_firmware	2288
	qualcomm_205_mobile_platform_firmware	2289
	qualcomm_215_mobile_platform_firmware	2290
	qualcomm_video_collaboration_vc1_platform_firmware	2291
	qualcomm_video_collaboration_vc3_platform_firmware	2294
	qualcomm_video_collaboration_vc5_platform_firmware	2297
	robotics_rb3_platform_firmware	2300
	robotics_rb5_platform_firmware	2301
	sa4150p_firmware	2305
	sa4155p_firmware	2308
	sa6145p_firmware	2311
	sa6150p_firmware	2315
	sa6155p_firmware	2320
	sa6155_firmware	2324
	sa8145p_firmware	2326
	sa8150p_firmware	2330
	sa8155p_firmware	2335
	sa8155_firmware	2339
	sa8195p_firmware	2342
	sa8255p_firmware	2346
	sa8295p_firmware	2350
	sa8540p_firmware	2353

Vendor	Product	Page Number
Qualcomm	sa9000p_firmware	2354
	sc8180x\+sdx55_firmware	2355
	sd460_firmware	2356
	sd626_firmware	2358
	sd660_firmware	2358
	sd662_firmware	2361
	sd670_firmware	2362
	sd675_firmware	2364
	sd730_firmware	2366
	sd820_firmware	2368
	sd821_firmware	2369
	sd835_firmware	2369
	sd855_firmware	2370
	sd865_5g_firmware	2373
	sd888_firmware	2376
	sdm429w_firmware	2379
	sdx20m_firmware	2380
	sdx55_firmware	2380
	sdx57m_firmware	2383
	sdx65m_firmware	2384
	sd_455_firmware	2385
	sd_675_firmware	2386
	sd_8cx_firmware	2388
	sd_8_gen1_5g_firmware	2389
	sg4150p_firmware	2391
	sg8275p_firmware	2394
	sm4125_firmware	2396
	sm4450_firmware	2398
	sm6250p_firmware	2399
	sm6250_firmware	2401
	sm7250p_firmware	2403
	sm7315_firmware	2406

Vendor	Product	Page Number
Qualcomm	sm7325p_firmware	2409
	sm8550p_firmware	2412
	smart_audio_200_platform_firmware	2415
	smart_audio_400_platform_firmware	2416
	smart_display_200_platform_firmware	2419
	snapdragon_1100_wearable_platform_firmware	2420
	snapdragon_1200_wearable_platform_firmware	2420
	snapdragon_208_processor_firmware	2421
	snapdragon_210_processor_firmware	2422
	snapdragon_212_mobile_platform_firmware	2422
	snapdragon_425_mobile_platform_firmware	2423
	snapdragon_427_mobile_platform_firmware	2424
	snapdragon_429_mobile_platform_firmware	2425
	snapdragon_430_mobile_platform_firmware	2426
	snapdragon_435_mobile_platform_firmware	2427
	snapdragon_439_mobile_platform_firmware	2427
	snapdragon_450_mobile_platform_firmware	2428
	snapdragon_460_mobile_platform_firmware	2429
	snapdragon_480\+_5g_mobile_platform_firmware	2432
	snapdragon_480_5g_mobile_platform_firmware	2436
	snapdragon_4_gen_1_mobile_platform_firmware	2440
	snapdragon_4_gen_2_mobile_platform_firmware	2443
	snapdragon_625_mobile_platform_firmware	2444
	snapdragon_626_mobile_platform_firmware	2445
	snapdragon_630_mobile_platform_firmware	2446
	snapdragon_632_mobile_platform_firmware	2447
	snapdragon_636_mobile_platform_firmware	2448
	snapdragon_660_mobile_platform_firmware	2449

Vendor	Product	Page Number
Qualcomm	snapdragon_662_mobile_platform_firmware	2452
	snapdragon_665_mobile_platform_firmware	2454
	snapdragon_670_mobile_platform_firmware	2457
	snapdragon_675_mobile_platform_firmware	2459
	snapdragon_678_mobile_platform_firmware	2462
	snapdragon_680_4g_mobile_platform_firmware	2465
	snapdragon_685_4g_mobile_platform_firmware	2469
	snapdragon_690_5g_mobile_platform_firmware	2474
	snapdragon_695_5g_mobile_platform_firmware	2477
	snapdragon_710_mobile_platform_firmware	2481
	snapdragon_712_mobile_platform_firmware	2482
	snapdragon_720g_mobile_platform_firmware	2484
	snapdragon_730g_mobile_platform_firmware	2486
	snapdragon_730_mobile_platform_firmware	2489
	snapdragon_732g_mobile_platform_firmware	2492
	snapdragon_750g_5g_mobile_platform_firmware	2494
	snapdragon_765g_5g_mobile_platform_firmware	2497
	snapdragon_765_5g_mobile_platform_firmware	2501
	snapdragon_768g_5g_mobile_platform_firmware	2504
	snapdragon_778g\+_5g_mobile_platform_firmware	2508
	snapdragon_778g_5g_mobile_platform_firmware	2512
	snapdragon_780g_5g_mobile_platform_firmware	2515
	snapdragon_782g_mobile_platform_firmware	2519
	snapdragon_7c\+_gen_3_compute_firmware	2522

Vendor	Product	Page Number
Qualcomm	snapdragon_7c_compute_platform_firmware	2526
	snapdragon_7c_gen_2_compute_platform_firmware	2528
	snapdragon_808_processor_firmware	2530
	snapdragon_810_processor_firmware	2530
	snapdragon_820_automotive_platform_firmware	2530
	snapdragon_820_mobile_platform_firmware	2532
	snapdragon_821_mobile_platform_firmware	2533
	snapdragon_835_mobile_pc_platform_firmware	2534
	snapdragon_845_mobile_platform_firmware	2536
	snapdragon_850_mobile_compute_platform_firmware	2537
	snapdragon_855\+\/860_mobile_platform_firmware	2539
	snapdragon_855_mobile_platform_firmware	2542
	snapdragon_865\+_5g_mobile_platform_firmware	2545
	snapdragon_865_5g_mobile_platform_firmware	2549
	snapdragon_870_5g_mobile_platform_firmware	2552
	snapdragon_888\+_5g_mobile_platform_firmware	2556
	snapdragon_888_5g_mobile_platform_firmware	2560
	snapdragon_8cx_compute_platform_firmware	2564
	snapdragon_8cx_gen_2_5g_compute_platform_firmware	2566
	snapdragon_8cx_gen_3_compute_platform_firmware	2568
	snapdragon_8c_compute_platform_firmware	2570
	snapdragon_8\+_gen_1_mobile_platform_firmware	2572

Vendor	Product	Page Number
Qualcomm	snapdragon_8\+_gen_2_mobile_platform_firmware	2575
	snapdragon_8_gen_1_mobile_platform_firmware	2577
	snapdragon_8_gen_2_mobile_platform_firmware	2580
	snapdragon_ar2_gen_1_platform_firmware	2583
	snapdragon_auto_4g_modem_firmware	2585
	snapdragon_auto_5g_modem-rf_firmware	2587
	snapdragon_w5\+_gen_1_wearable_platform_firmware	2591
	snapdragon_wear_1300_platform_firmware	2596
	snapdragon_wear_2100_platform_firmware	2597
	snapdragon_wear_2500_platform_firmware	2598
	snapdragon_wear_3100_platform_firmware	2599
	snapdragon_wear_4100\+_platform_firmware	2600
	snapdragon_x12_lte_modem_firmware	2602
	snapdragon_x20_lte_modem_firmware	2604
	snapdragon_x24_lte_modem_firmware	2605
	snapdragon_x50_5g_modem-rf_system_firmware	2607
	snapdragon_x55_5g_modem-rf_system_firmware	2610
	snapdragon_x5_lte_modem_firmware	2614
	snapdragon_x65_5g_modem-rf_system_firmware	2615
	snapdragon_x70_modem-rf_system_firmware	2618
	snapdragon_x75_5g_modem-rf_system_firmware	2620
	snapdragon_xr1_platform_firmware	2622
	snapdragon_xr2\+_gen_1_platform_firmware	2623
	snapdragon_xr2_5g_platform_firmware	2626
	ssg2115p_firmware	2630
	ssg2125p_firmware	2632

Vendor	Product	Page Number
Qualcomm	sw5100p_firmware	2634
	sw5100_firmware	2639
	sxr1120_firmware	2643
	sxr1230p_firmware	2645
	sxr2130_firmware	2647
	sxr2230p_firmware	2650
	vision_intelligence_100_platform_firmware	2652
	vision_intelligence_200_platform_firmware	2653
	vision_intelligence_300_platform_firmware	2654
	vision_intelligence_400_platform_firmware	2656
	wcd9306_firmware	2658
	wcd9326_firmware	2659
	wcd9330_firmware	2662
	wcd9335_firmware	2664
	wcd9340_firmware	2668
	wcd9341_firmware	2671
	wcd9360_firmware	2676
	wcd9370_firmware	2678
	wcd9371_firmware	2683
	wcd9375_firmware	2685
	wcd9380_firmware	2690
	wcd9385_firmware	2695
	wcd9390_firmware	2700
	wcd9395_firmware	2702
	wcn3610_firmware	2705
	wcn3615_firmware	2707
	wcn3620_firmware	2709
	wcn3660b_firmware	2710
	wcn3660_firmware	2713
	wcn3680b_firmware	2714
	wcn3680_firmware	2717
	wcn3910_firmware	2718

Vendor	Product	Page Number
Qualcomm	wcn3950_firmware	2721
	wcn3980_firmware	2725
	wcn3988_firmware	2730
	wcn3990_firmware	2735
	wcn3999_firmware	2739
	wcn6740_firmware	2741
	wsa8810_firmware	2744
	wsa8815_firmware	2749
	wsa8830_firmware	2754
	wsa8832_firmware	2759
	wsa8835_firmware	2762
	wsa8840_firmware	2768
	wsa8845h_firmware	2770
	wsa8845_firmware	2772
Redhat	enterprise_linux	2775
Samsung	android	2781
Tenda	a18_firmware	2785
	ax12_firmware	2785
	ax1803_firmware	2786
	ax3_firmware	2791
	i29_firmware	2791
totolink	lr1200gb_firmware	2792
	n200re_firmware	2796
	n350rt_firmware	2799
	nr1800x_firmware	2802
	t6_firmware	2803
	x2000r_firmware	2805
Trendnet	tv-ip1314pi_firmware	2806
uniwayinfo	uw-101x_firmware	2807
	uw-301vpw_firmware	2809
	uw-302vp_firmware	2811
	uw-311vpw_firmware	2813

Vendor	Product	Page Number
uniwayinfo	uw-323dac_firmware	2814
XEN	xen	2816
ZTE	red_magic_8_pro_firmware	2828
	zxcloud_irai_firmware	2828

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: abocms					
Product: abo.cms					
Affected Version(s): 5.9.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jan-2024	9.8	SQL Injection vulnerability in ABO.CMS v.5.9.3, allows remote attackers to execute arbitrary code via the d parameter in the Documents module. **CVE ID : CVE-2023-46953**	N/A	A-ABO-ABO.-290124/1
Vendor: Acme					
Product: ultra_mini_httpd					
Affected Version(s): 1.21					
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in ACME Ultra Mini HTTPd 1.21. It has been classified as problematic. This affects an unknown part of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is	N/A	A-ACM-ULTR-290124/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-249819. **CVE ID : CVE-2024-0263**		
Vendor: acumos					
Product: design_studio					
Affected Version(s): * Up to (excluding) 2.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	A vulnerability, which was classified as problematic, was found in Acumos Design Studio up to 2.0.7. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.0.8 is able to address this issue. The name of the patch is 0df8a5e8722188744973168648e4c74c69ce67fd. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-249420.	https://github.com/acumos/design-studio/commit/0df8a5e8722188744973168648e4c74c69ce67fd	A-ACU-DESI-290124/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2018-25097		
Vendor: Adobe					
Product: substance_3d_stager					
Affected Version(s): * Up to (including) 2.1.3					
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20710**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	A-ADO-SUBS-290124/4
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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/substance3d_stager/apsb24-06.html	A-ADO-SUBS-290124/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-20711**		
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20712**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	A-ADO-SUBS-290124/6
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	A-ADO-SUBS-290124/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2024-20713**		
Vendor: advancedcustomfields					
Product: advanced_custom_fields					
Affected Version(s): From (including) 3.1.1 Up to (including) 6.0.2					
N/A	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Engine Advanced Custom Fields (ACF).This issue affects Advanced Custom Fields (ACF): from 3.1.1 through 6.0.2. **CVE ID : CVE-2022-40696**	N/A	A-ADV-ADVA-290124/8
Vendor: ajexperience					
Product: 404_solution					
Affected Version(s): * Up to (including) 2.33.0					
Insertion of Sensitive Information into Log File	05-Jan-2024	5.3	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Aaron J 404 Solution.This issue affects 404 Solution: from n/a through 2.33.0. **CVE ID : CVE-2023-52146**	N/A	A-AJE-404_-290124/9
Vendor: alekseykurepin					
Product: pico_http_server_in_c					
Affected Version(s): * Up to (including) 2021-04-02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Jan-2024	9.8	route in main.c in Pico HTTP Server in C through f3b69a6 has an sprintf stack-based buffer overflow via a long URI, leading to remote code execution. **CVE ID : CVE-2024-22087**	N/A	A-ALE-PICO-290124/10
Vendor: Amazon					
Product: ion					
Affected Version(s): * Up to (excluding) 1.10.5					
Allocation of Resources Without Limits or Throttling	03-Jan-2024	7.5	Amazon Ion is a Java implementation of the Ion data notation. Prior to version 1.10.5, a potential denial-of-service issue exists in `ion-java` for applications that use `ion-java` to deserialize Ion text encoded data, or deserialize Ion text or binary encoded data into the `IonValue` model and then invoke certain `IonValue` methods on that in-memory representation. An actor could craft Ion data that, when loaded by the affected application and/or processed using	https://github.com/amazon-ion/ion-java/security/advisories/GHSA-264p-99wq-f4j6	A-AMA-ION-290124/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `IonValue` model, results in a `StackOverflowError` originating from the `ion-java` library. The patch is included in `ion-java` 1.10.5. As a workaround, do not load data which originated from an untrusted source or that could have been tampered with. **CVE ID : CVE-2024-21634**		
Vendor: antonbond					
Product: woocommerce_tranzila_payment_gateway					
Affected Version(s): * Up to (including) 1.0.8					
Deserialization of Untrusted Data	08-Jan-2024	9.8	Deserialization of Untrusted Data vulnerability in Anton Bond Woocommerce Tranzila Payment Gateway.This issue affects Woocommerce Tranzila Payment Gateway: from n/a through 1.0.8. **CVE ID : CVE-2023-52218**	N/A	A-ANT-WOOC-290124/12
Vendor: Apache					
Product: axis					
Affected Version(s): * Up to (including) 1.3					
Server-Side Request	06-Jan-2024	7.2	** UNSUPPORTED WHEN ASSIGNED ** Improper Input Validation	https://github.com/apache/axis-axis1-java/commit/6	A-APA-AXIS-290124/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			vulnerability in Apache Axis allowed users with access to the admin service to perform possible SSRF This issue affects Apache Axis: through 1.3. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. Alternatively you could use a build of Axis with the patch from https://github.com/apache/axis-axis1-java/commit/685c309febc64aa393b2d64a05f90e7eb9f73e06 applied. The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome. **CVE ID : CVE-2023-51441**	85c309febc64aa393b2d64a05f90e7eb9f73e06, https://lists.apache.org/thread/8nrm5thop8f82pglx4o0jg8wmvy6d9yd	
Product: inlong					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.10.0					
Improper Control of Generation of Code ('Code Injection')	03-Jan-2024	9.8	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.9.0, which could lead to Remote Code Execution. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9329 **CVE ID : CVE-2023-51784**	https://lists.apache.org/thread/4nxbyl6mh5jgh0plk0qposbxwn6w9h8j	A-APA-INLO-290124/14
Affected Version(s): From (including) 1.7.0 Up to (including) 1.9.0					
Deserialization of Untrusted Data	03-Jan-2024	7.5	Deserialization of Untrusted Data vulnerability in Apache InLong.This issue affects Apache InLong: from 1.7.0 through 1.9.0, the attackers can make a arbitrary file read attack using mysql driver. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it.	https://lists.apache.org/thread/g0yjmtjqvp8bnf1j0tdsk0nhfozjdjno	A-APA-INLO-290124/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[1] https://github.com/apache/inlong/pull/9331 **CVE ID : CVE-2023-51785**		
Vendor: apiida					
Product: api_gateway_manager					
Affected Version(s): 2023.02.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	APIIDA API Gateway Manager for Broadcom Layer7 v2023.2 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-50092**	N/A	A-API-API_-290124/16
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	6.1	APIIDA API Gateway Manager for Broadcom Layer7 v2023.2.2 is vulnerable to Host Header Injection. **CVE ID : CVE-2023-50093**	N/A	A-API-API_-290124/17
Vendor: apktool					
Product: apktool					
Affected Version(s): * Up to (excluding) 2.9.2					
Improper Limitation of a Pathname to a Restricted Directory	03-Jan-2024	7.8	Apktool is a tool for reverse engineering Android APK files. In versions 2.9.1 and prior, Apktool infers resource	https://github.com/iBotPeaches/Apktool/commit/d348c43b24a9de350ff6e5bd610545a10c1fc712,	A-APK-APKT-290124/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			files' output path according to their resource names which can be manipulated by attacker to place files at desired location on the system Apktool runs on. Affected environments are those in which an attacker may write/overwrite any file that user has write access, and either user name is known or cwd is under user folder. Commit d348c43b24a9de350ff6e5bd610545a10c1fc712 contains a patch for this issue. **CVE ID : CVE-2024-21633**	https://github.com/iBotPeaches/Apktool/security/advisories/GHSA-2hqv-2xv4-5h5w	
Vendor: apollo13themes					
Product: apollo13_framework_extensions					
Affected Version(s): * Up to (including) 1.9.1					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Apollo13Themes Apollo13 Framework Extensions.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.1.	N/A	A-APO-APOL-290124/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51539		
Vendor: appwrite					
Product: command_line_interface					
Affected Version(s): * Up to (excluding) 3.0.0					
Use of Hard-coded Credentials	09-Jan-2024	5.5	In Appwrite CLI before 3.0.0, when using the login command, the credentials of the Appwrite user are stored in a ~/.appwrite/prefs.json file with 0644 as UNIX permissions. Any user of the local system can access those credentials. **CVE ID : CVE-2023-50974**	N/A	A-APP-COMM-290124/20
Vendor: ARM					
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r37p0 Up to (including) r40p0					
Use After Free	08-Jan-2024	5.5	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU processing operations to gain access to already freed memory. This issue affects Valhall GPU Kernel Driver: from r37p0 through r40p0.	https://developer.arm.com/Arm Security Center/Mali GPU Driver Vulnerabilities	A-ARM-VALH-290124/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5091		
Vendor: Automattic					
Product: woocommerce_stripe					
Affected Version(s): * Up to (including) 7.6.1					
Authorization Bypass Through User-Controlled Key	05-Jan-2024	9.8	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce Stripe Payment Gateway.This issue affects WooCommerce Stripe Payment Gateway: from n/a through 7.6.1. **CVE ID : CVE-2023-51502**	N/A	A-AUT-WOOC-290124/22
Vendor: ava					
Product: teaching_video_application_service_platform					
Affected Version(s): 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jan-2024	6.1	Cross Site Scripting (XSS) vulnerability in AVA teaching video application service platform version 3.1, allows remote attackers to execute arbitrary code via a crafted script to ajax.aspx. **CVE ID : CVE-2023-50609**	N/A	A-AVA-TEAC-290124/23
Vendor: averta					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: depicter_slider					
Affected Version(s): * Up to (including) 2.0.6					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	4.3	The Depicter Slider – Responsive Image Slider, Video Slider & Post Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.6. This is due to missing or incorrect nonce validation on the 'save' function. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. CVE-2023-51491 appears to be a duplicate of this issue. **CVE ID : CVE-2023-6493**	https://plugins.trac.wordpress.org/changeset/3013596/depicter/trunk/app/src/WordPress/Settings/Settings.php	A-AVE-DEPI-290124/24
Vendor: backupbliss					
Product: backup_migration					
Affected Version(s): * Up to (excluding) 1.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jan-2024	7.5	The Backup Migration WordPress plugin before 1.3.6 stores in-progress backups information in easy to find, publicly-accessible files, which may allow attackers monitoring those to leak sensitive information from the site's backups. **CVE ID : CVE-2023-6271**	N/A	A-BAC-BACK-290124/25
Product: clone					
Affected Version(s): * Up to (excluding) 2.4.3					
N/A	08-Jan-2024	7.5	The Clone WordPress plugin before 2.4.3 uses buffer files to store in-progress backup informations, which is stored at a publicly accessible, statically defined file path. **CVE ID : CVE-2023-6750**	N/A	A-BAC-CLON-290124/26
Vendor: basixonline					
Product: nex-forms					
Affected Version(s): * Up to (including) 8.5.2					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms – Ultimate Form Builder – Contact forms and much	N/A	A-BAS-NEX--290124/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			more.This issue affects NEX-Forms – Ultimate Form Builder – Contact forms and much more: from n/a through 8.5.2. **CVE ID : CVE-2023-52120**		
Vendor: bladex					
Product: springblade					
Affected Version(s): * Up to (including) 3.7.0					
Missing Authorization	02-Jan-2024	9.8	An issue in SpringBlade v.3.7.0 and before allows a remote attacker to escalate privileges via the lack of permissions control framework. **CVE ID : CVE-2023-47458**	N/A	A-BLA-SPRI-290124/28
Vendor: blueastral					
Product: page_builder					
Affected Version(s): _live_composer Up to (including) 1.5.25					
Deserialization of Untrusted Data	08-Jan-2024	7.2	Deserialization of Untrusted Data vulnerability in Live Composer Team Page Builder: Live Composer live-composer-page-builder.This issue affects Page Builder: Live Composer: from n/a through 1.5.25. **CVE ID : CVE-2023-52206**	N/A	A-BLU-PAGE-290124/29
Vendor: boazsegev					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: iodine					
Affected Version(s): * Up to (including) 0.7.33					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	7.5	Path traversal in the static file service in Iodine less than 0.7.33 allows an unauthenticated, remote attacker to read files outside the public folder via malicious URLs. **CVE ID : CVE-2024-22050**	https://github.com/advisories/GHSA-85rf-xh54-whp3, https://github.com/boazsegev/iodine/commit/5558233fb7defda706b4f9c87c17759705949889, https://github.com/boazsegev/iodine/security/advisories/GHSA-85rf-xh54-whp3	A-BOA-IODI-290124/30
Vendor: bowo					
Product: debug_log_manager					
Affected Version(s): * Up to (excluding) 2.3.0					
Missing Authorization	08-Jan-2024	7.5	The Debug Log Manager WordPress plugin before 2.3.0 contains a Directory listing vulnerability was discovered, which allows you to download the debug log without authorization and gain access to sensitive data **CVE ID : CVE-2023-6383**	N/A	A-BOW-DEBU-290124/31
Vendor: bplugins					
Product: html5_video_player					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.5.19					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2024	5.4	The Html5 Video Player WordPress plugin before 2.5.19 does not sanitise and escape some of its player settings, which combined with missing capability checks around the plugin could allow any authenticated users, such as low as subscribers to perform Stored Cross-Site Scripting attacks against high privilege users like admins **CVE ID : CVE-2023-6485**	N/A	A-BPL-HTML-290124/32
Vendor: briandgoad					
Product: ptypeconverter					
Affected Version(s): * Up to (including) 0.2.8.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brian D. Goad pTypeConverter.This issue affects pTypeConverter: from n/a through 0.2.8.1.	N/A	A-BRI-PTYP-290124/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52201		
Vendor: buy-addons					
Product: bazoom_magnifier					
Affected Version(s): * Up to (including) 1.0.16					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jan-2024	9.8	SQL Injection vulnerability in Buy Addons baproductzoommagnifier module for PrestaShop versions 1.0.16 and before, allows remote attackers to escalate privileges and gain sensitive information via BaproductzoommagnifierZoomModuleFrontController::run() method. **CVE ID : CVE-2023-50027**	https://security.friendsofpresta.org/modules/2023/12/19/baproductzoommagnifier.html	A-BUY-BAZO-290124/34
Vendor: Canonical					
Product: snapd					
Affected Version(s): * Up to (excluding) 2.61.1					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	A-CAN-SNAP-290124/35
Vendor: Cesanta					
Product: mjs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.20.0					
N/A	02-Jan-2024	7.5	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_getretvalpos function in the msj.c file. **CVE ID : CVE-2023-49549**	https://github.com/cesanta/mjs/issues/251	A-CES-MJS-290124/36
N/A	02-Jan-2024	7.5	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs+0x4ec508 component. **CVE ID : CVE-2023-49550**	https://github.com/cesanta/mjs/issues/252	A-CES-MJS-290124/37
N/A	02-Jan-2024	7.5	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_op_json_parse function in the msj.c file. **CVE ID : CVE-2023-49551**	https://github.com/cesanta/mjs/issues/257	A-CES-MJS-290124/38
Out-of-bounds Read	02-Jan-2024	7.5	An Out of Bounds Write in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_op_json_stringify function in the msj.c file. **CVE ID : CVE-2023-49552**	https://github.com/cesanta/mjs/issues/256	A-CES-MJS-290124/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	An issue in Cesanta mjs 2.20.0 allows a remote attacker to cause a denial of service via the mjs_destroy function in the msj.c file. **CVE ID : CVE-2023-49553**	https://github.com/cesanta/mjs/issues/253	A-CES-MJS-290124/40
Vendor: cformsii_project					
Product: cformsii					
Affected Version(s): * Up to (including) 15.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliver Seidel, Bastian Germann cformsII allows Stored XSS.This issue affects cformsII: from n/a through 15.0.5. **CVE ID : CVE-2023-52203**	N/A	A-CFO-CFOR-290124/41
Vendor: chanzhaoyu					
Product: chatgpt_web					
Affected Version(s): 2.11.1					
Improper Neutralization of Input During Web Page	08-Jan-2024	6.1	A vulnerability, which was classified as problematic, has been found in Chanzhaoyu	N/A	A-CHA-CHAT-290124/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			chatgpt-web 2.11.1. This issue affects some unknown processing. The manipulation of the argument Description with the input <image src onerror=prompt(document.domain)> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249779. **CVE ID : CVE-2023-7215**		
Vendor: chendotjs					
Product: lotos_webserver					
Affected Version(s): * Up to (including) 0.1.1					
Use After Free	05-Jan-2024	9.8	Lotos WebServer through 0.1.1 (commit 3eb36cc) has a use-after-free in buffer_avail() at buffer.h via a long URI, because realloc is mishandled. **CVE ID : CVE-2024-22088**	https://github.com/chendotjs/lotos/issues/7	A-CHE-LOTO-290124/43
Vendor: cleantalk					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: spam_protection\,_antispam\,_firewall					
Affected Version(s): * Up to (including) 6.20					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in ?leanTalk - Anti-Spam Protection Spam protection, Anti-Spam, FireWall by CleanTalk.This issue affects Spam protection, Anti-Spam, FireWall by CleanTalk: from n/a through 6.20. **CVE ID : CVE-2023-51535**	N/A	A-CLE-SPAM-290124/44
Vendor: cloudflare					
Product: zlib					
Affected Version(s): * Up to (excluding) 2023-11-16					
Out-of-bounds Write	04-Jan-2024	5.5	Cloudflare version of zlib library was found to be vulnerable to memory corruption issues affecting the deflation algorithm implementation (deflate.c). The issues resulted from improper input validation and heap-based buffer overflow. A local attacker could exploit the problem during	https://github.com/cloudflare/zlib/security/advisories/GHSA-vww9-j87r-4cqh	A-CLO-ZLIB-290124/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compression using a crafted malicious file potentially leading to denial of service of the software. Patches: The issue has been patched in commit 8352d10 https://github.com/cloudflare/zlib/commit/8352d108c05db1bdc5ac3bdf834dad641694c13c . The upstream repository is not affected. **CVE ID : CVE-2023-6992**		
Vendor: code-projects					
Product: simple_online_hotel_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be	N/A	A-COD-SIMP-290124/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250126 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0359**		
Vendor: codeastro					
Product: internet_banking_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	02-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in CodeAstro Internet Banking System up to 1.0. This issue affects some unknown processing of the file pages_account.php of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249509 was assigned to this vulnerability.	N/A	A-COD-INTE-290124/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0194		
Vendor: Codecabin					
Product: wp_go_maps					
Affected Version(s): * Up to (excluding) 9.0.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	The WP Go Maps (formerly WP Google Maps) WordPress plugin before 9.0.28 does not properly protect most of its REST API routes, which attackers can abuse to store malicious HTML/Javascript on the site. **CVE ID : CVE-2023-6627**	N/A	A-COD-WP_G-290124/48
Vendor: coderex					
Product: wp_vr					
Affected Version(s): * Up to (excluding) 8.3.15					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	6.1	The WP VR WordPress plugin before 8.3.15 does not authorisation and CSRF in a function hooked to admin_init, allowing unauthenticated users to downgrade the plugin, thus leading to Reflected or Stored XSS, as previous versions have such vulnerabilities.	N/A	A-COD-WP_V-290124/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6529		
Vendor: codexonics					
Product: prime_mover					
Affected Version(s): * Up to (excluding) 1.9.3					
N/A	08-Jan-2024	7.5	The Migrate WordPress Website & Backups WordPress plugin before 1.9.3 does not prevent directory listing in sensitive directories containing export files. **CVE ID : CVE-2023-6505**	N/A	A-COD-PRIM-290124/50
Vendor: collectiveidea					
Product: audited					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 5.3.3					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Jan-2024	3.1	A race condition exists in Audited 4.0.0 to 5.3.3 that can result in an authenticated user to cause audit log entries to be attributed to another user. **CVE ID : CVE-2024-22047**	https://github.com/collectiveidea/audited/issues/601, https://github.com/collectiveidea/audited/pull/669, https://github.com/collectiveidea/audited/pull/671, https://github.com/collectiveidea/audited/security/advisories/GHSA-hjp3-5g2q-7jww	A-COL-AUDI-290124/51
Vendor: constantcontact					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: constant_contact_forms					
Affected Version(s): * Up to (including) 2.4.2					
N/A	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Constant Contact Constant Contact Forms.This issue affects Constant Contact Forms: from n/a through 2.4.2. **CVE ID : CVE-2023-52208**	N/A	A-CON-CONS-290124/52
Vendor: coolplugins					
Product: events_shortcodes_for_the_events_calendar					
Affected Version(s): * Up to (including) 2.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cool Plugins Events Shortcodes For The Events Calendar.This issue affects Events Shortcodes For The Events Calendar: from n/a through 2.3.1.	N/A	A-COO-EVEN-290124/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52142		
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.9.6					
N/A	03-Jan-2024	8.8	Craft is a content management system. This is a potential moderate impact, low complexity privilege escalation vulnerability in Craft starting in 3.x prior to 3.9.6 and 4.x prior to 4.4.16 with certain user permissions setups. This has been fixed in Craft 4.4.16 and Craft 3.9.6. Users should ensure they are running at least those versions. **CVE ID : CVE-2024-21622**	https://github.com/craftcms/cms/commit/76caf9af07d9964be0fd362772223be6a5f5b6aa, https://github.com/craftcms/cms/commit/be81eb653d633833f2ab22510794abb6bb9c0843, https://github.com/craftcms/cms/pull/13931, https://github.com/craftcms/cms/pull/13932	A-CRA-CRAF-290124/54
Affected Version(s): From (including) 4.0.0 Up to (including) 4.5.15					
N/A	03-Jan-2024	8.8	Craft is a content management system. This is a potential moderate impact, low complexity privilege escalation vulnerability in Craft starting in 3.x prior to 3.9.6 and 4.x prior to 4.4.16 with certain user permissions setups. This has	https://github.com/craftcms/cms/commit/76caf9af07d9964be0fd362772223be6a5f5b6aa, https://github.com/craftcms/cms/commit/be81eb653d633833f2ab22510794abb6bb9c0843, https://github.c	A-CRA-CRAF-290124/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been fixed in Craft 4.4.16 and Craft 3.9.6. Users should ensure they are running at least those versions. **CVE ID : CVE-2024-21622**	om/craftcms/cms/pull/13931, https://github.com/craftcms/cms/pull/13932	
Vendor: daan					
Product: omgf					
Affected Version(s): * Up to (excluding) 5.7.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	5.4	The OMGF | GDPR/DSGVO Compliant, Faster Google Fonts. Easy. plugin for WordPress is vulnerable to unauthorized modification of data and Stored Cross-Site Scripting due to a missing capability check on the update_settings() function hooked via admin_init in all versions up to, and including, 5.7.9. This makes it possible for unauthenticated attackers to update the plugin's settings which can be used to inject Cross-Site Scripting payloads and delete entire directories. PLease note there were	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3008876%40host-webfonts-local&new=3008876%40host-webfonts-local&sfp_email=&sfph_mail=	A-DAA-OMGF-290124/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			several attempted patched, and we consider 5.7.10 to be the most sufficiently patched. **CVE ID : CVE-2023-6600**		
Vendor: dataiku					
Product: data_science_studio					
Affected Version(s): * Up to (excluding) 11.4.5					
Improper Authentication	09-Jan-2024	9.8	Dataiku DSS before 11.4.5 and 12.4.1 has Incorrect Access Control that could lead to a full authentication bypass. **CVE ID : CVE-2023-51717**	https://doc.dataiku.com/dss/latest/security/advisories/dsa-2023-010.html	A-DAT-DATA-290124/57
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.4.1					
Improper Authentication	09-Jan-2024	9.8	Dataiku DSS before 11.4.5 and 12.4.1 has Incorrect Access Control that could lead to a full authentication bypass. **CVE ID : CVE-2023-51717**	https://doc.dataiku.com/dss/latest/security/advisories/dsa-2023-010.html	A-DAT-DATA-290124/58
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): * Up to (including) 5.7.112					
Unrestricted Upload of File with Dangerous Type	07-Jan-2024	9.8	A vulnerability classified as critical has been found in DeDeCMS up to 5.7.112. Affected is an unknown	N/A	A-DED-DEDE-290124/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the file file_class.php of the component Backend. The manipulation 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-249768. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7212**		
Vendor: demon1a					
Product: discord-recon					
Affected Version(s): * Up to (excluding) 0.0.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jan-2024	8.8	Discord-Recon is a Discord bot created to automate bug bounty recon, automated scans and information gathering via a discord server. Discord-Recon is vulnerable to remote code execution. An attacker is able to execute shell commands in the	https://github.com/DEMON1A/Discord-Recon/commit/f9cb0f67177f5e2f1022295ca8e641e47837ec7a, https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-fjcj-g7x8-4rp7	A-DEM-DISC-290124/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server without having an admin role. This vulnerability has been fixed in version 0.0.8. **CVE ID : CVE-2024-21663**		
Affected Version(s): 0.0.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Jan-2024	8.8	Discord-Recon is a Discord bot created to automate bug bounty recon, automated scans and information gathering via a discord server. Discord-Recon is vulnerable to remote code execution. An attacker is able to execute shell commands in the server without having an admin role. This vulnerability has been fixed in version 0.0.8. **CVE ID : CVE-2024-21663**	https://github.com/DEMON1A/Discord-Recon/commit/f9cb0f67177f5e2f1022295ca8e641e47837ec7a, https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-fjcj-g7x8-4rp7	A-DEM-DISC-290124/61
Vendor: diaconou					
Product: encodedid					
Affected Version(s): \\					
Allocation of Resources Without	04-Jan-2024	7.5	encoded_id-rails versions before 1.0.0.beta2 are affected by an	https://github.com/stevegeek/encoded_id-rails/commit/af	A-DIA-ENCO-290124/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			uncontrolled resource consumption vulnerability. A remote and unauthenticated attacker might cause a denial of service condition by sending an HTTP request with an extremely long "id" parameter. **CVE ID : CVE-2024-0241**	a495a77b8a21ad582611f9cdc2081dc4018b91, https://github.com/stevegeek/encoded_id-rails/security/advisories/GHSA-3px7-jm2p-6h2c	
Affected Version(s): \\ Up to (excluding) 1.0.0					
Allocation of Resources Without Limits or Throttling	04-Jan-2024	7.5	encoded_id-rails versions before 1.0.0.beta2 are affected by an uncontrolled resource consumption vulnerability. A remote and unauthenticated attacker might cause a denial of service condition by sending an HTTP request with an extremely long "id" parameter. **CVE ID : CVE-2024-0241**	https://github.com/stevegeek/encoded_id-rails/commit/afa495a77b8a21ad582611f9cdc2081dc4018b91, https://github.com/stevegeek/encoded_id-rails/security/advisories/GHSA-3px7-jm2p-6h2c	A-DIA-ENCO-290124/63
Vendor: doofinder					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: doofinder					
Affected Version(s): * Up to (including) 2.0.33					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Doofinder Doofinder WP & WooCommerce Search.This issue affects Doofinder WP & WooCommerce Search: from n/a through 2.0.33. **CVE ID : CVE-2023-51678**	N/A	A-DOO-DOOF-290124/64
Vendor: dzzoffice					
Product: dzzoffice					
Affected Version(s): 2.01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Jan-2024	6.5	SQL Injection vulnerability in Dzzoffice version 2.01, allows remote attackers to obtain sensitive information via the doobj and doevent parameters in the Network Disk backend module. **CVE ID : CVE-2023-39853**	N/A	A-DZZ-DZZO-290124/65
Vendor: Easyxdm					
Product: easyxdm					
Affected Version(s): 2.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	easyXDM 2.5 allows XSS via the xdm_e parameter. **CVE ID : CVE-2023-27739**	N/A	A-EAS-EASY-290124/66
Vendor: ekolbilisim					
Product: web_sablonu_yazilimi					
Affected Version(s): * Up to (including) 20231215					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jan-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ekol Informatics Website Template allows SQL Injection.This issue affects Website Template: through 20231215. **CVE ID : CVE-2023-6436**	N/A	A-EKO-WEB_-290124/67
Vendor: engineers_online_portal_project					
Product: engineers_online_portal					
Affected Version(s): 1.0					
Insufficient Session Expiration	07-Jan-2024	7.5	A vulnerability, which was classified as problematic, was found in SourceCodester Engineers Online	N/A	A-ENG-ENGI-290124/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Portal 1.0. Affected is an unknown function of the file change_password_teacher.php of the component Password Change. The manipulation leads to session expiration. 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-249816. **CVE ID : CVE-2024-0260**		
Uncontrolled Resource Consumption	09-Jan-2024	6.5	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been classified as problematic. Affected is an unknown function of the component File Upload Handler. The manipulation leads to resource consumption. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-ENG-ENGI-290124/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-250116. **CVE ID : CVE-2024-0348**		
Insufficient Session Expiration	09-Jan-2024	6.5	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. VDB-250118 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0350**	N/A	A-ENG-ENGI-290124/70
Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	09-Jan-2024	5.3	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been declared as problematic. Affected by this	N/A	A-ENG-ENGI-290124/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is an unknown functionality. The manipulation leads to sensitive cookie without secure attribute. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-250117 was assigned to this vulnerability. **CVE ID : CVE-2024-0349**		
Weak Password Requirements	09-Jan-2024	3.7	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file signup_teacher.php. The manipulation of the argument Password leads to weak password requirements. The attack may be initiated remotely.	N/A	A-ENG-ENGI-290124/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250115. **CVE ID : CVE-2024-0347**		
Session Fixation	09-Jan-2024	3.5	A vulnerability classified as problematic has been found in SourceCodester Engineers Online Portal 1.0. This affects an unknown part. The manipulation leads to session fixiation. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250119.	N/A	A-ENG-ENGI-290124/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0351		
Vendor: Evernote					
Product: evernote					
Affected Version(s): 10.68.2					
N/A	09-Jan-2024	9.8	An issue in Evernote Evernote for MacOS v.10.68.2 allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeClilnspectArguments components. **CVE ID : CVE-2023-50643**	N/A	A-EVE-EVER-290124/74
Vendor: evm_project					
Product: evm					
Affected Version(s): * Up to (excluding) 0.41.1					
N/A	02-Jan-2024	7.5	Rust EVM is an Ethereum Virtual Machine interpreter. In `rust-evm`, a feature called `record_external_operation` was introduced, allowing library users to record custom gas changes. This feature can have some bogus interactions with the call stack. In particular, during finalization of a `CREATE` or	https://github.com/rust-ethereum/evm/commit/d8991ec727ad0fb64fe9957a3cd307387a6701e4, https://github.com/rust-ethereum/evm/pull/264, https://github.com/rust-ethereum/evm/security/advisories/GHSA-27wg-99g8-2v4v	A-EVM-EVM-290124/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CREATE2`, in the case that the substack execution happens successfully, `rust-evm` will first commit the substate, and then call `record_external_operation(Write(out_code.len()))`. If `record_external_operation` later fails, this error is returned to the parent call stack, instead of `Succeeded`. Yet, the substate commitment already happened. This causes smart contracts able to commit state changes, when the parent caller contract receives zero address (which usually indicates that the execution has failed). This issue only impacts library users with custom `record_external_operation` that returns errors. The issue is patched in release 0.41.1. No known workarounds are available.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21629		
Vendor: ewels					
Product: cpt_bootstrap_carousel					
Affected Version(s): * Up to (including) 1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Phil Ewels CPT Bootstrap Carousel allows Reflected XSS.This issue affects CPT Bootstrap Carousel: from n/a through 1.12. **CVE ID : CVE-2023-52196**	N/A	A-EWE-CPT_-290124/76
Vendor: fastify					
Product: reply-from					
Affected Version(s): * Up to (excluding) 9.6.0					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Jan-2024	7.5	fastify-reply-from is a Fastify plugin to forward the current HTTP request to another server. A reverse proxy server built with `@fastify/reply-from` could misinterpret the incoming body by passing an header	https://github.com/fastify/fastify-reply-from/security/advisories/GHSA-v2v2-hph8-q5xp	A-FAS-REPL-290124/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`ContentType: application/json ; charset=utf-8`. This can lead to bypass of security checks. This vulnerability has been patched in '@fastify/reply-from` version 9.6.0. **CVE ID : CVE-2023-51701**		
Vendor: fhs-opensource					
Product: iparking					
Affected Version(s): 1.5.22					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	9.8	A vulnerability classified as critical was found in fhs-opensource iparking 1.5.22.RELEASE. This vulnerability affects the function getData of the file src/main/java/com/xhb/pay/action/PayTempOrderAction.java. The manipulation 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-249868. **CVE ID : CVE-2024-0301**	N/A	A-FHS-IPAR-290124/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in fhs-opensource iparking 1.5.22.RELEASE. This issue affects some unknown processing of the file /vueLogin. The manipulation leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249869 was assigned to this vulnerability. **CVE ID : CVE-2024-0302**	N/A	A-FHS-IPAR-290124/79
Vendor: firefly-iii					
Product: firefly_iii					
Affected Version(s): * Up to (excluding) 6.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	6.1	Firefly III (aka firefly-iii) before 6.1.1 allows webhooks HTML Injection. **CVE ID : CVE-2024-22075**	N/A	A-FIR-FIRE-290124/80
Vendor: fit2cloud					
Product: cloudexplorer_lite					
Affected Version(s): 1.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	06-Jan-2024	7.8	Insecure Permissions vulnerability in fit2cloud Cloud Explorer Lite version 1.4.1, allow local attackers to escalate privileges and obtain sensitive information via the cloud accounts parameter. **CVE ID : CVE-2023-50612**	N/A	A-FIT-CLOU-290124/81
Vendor: floorsightsoftware					
Product: customer_portal					
Affected Version(s): * Up to (including) q3_2023					
Authorization Bypass Through User-Controlled Key	02-Jan-2024	7.5	An indirect Object Reference (IDOR) in the Order and Invoice pages in Floorsight Customer Portal Q3 2023 allows an unauthenticated remote attacker to view sensitive customer information. **CVE ID : CVE-2023-45893**	N/A	A-FLO-CUST-290124/82
Product: insight					
Affected Version(s): * Up to (including) q3_2023					
Authorization Bypass Through User-Controlled Key	02-Jan-2024	7.5	An issue discovered in the Order and Invoice pages in Floorsight Insights Q3 2023 allows an unauthenticated	N/A	A-FLO-INSI-290124/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to view sensitive customer information. **CVE ID : CVE-2023-45892**		
Vendor: flycms_project					
Product: flycms					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/userconfig_updagte. **CVE ID : CVE-2023-52072**	N/A	A-FLY-FLYC-290124/84
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/config_footer_updagte. **CVE ID : CVE-2023-52073**	N/A	A-FLY-FLYC-290124/85
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component system/site/webconfig_updagte. **CVE ID : CVE-2023-52074**	N/A	A-FLY-FLYC-290124/86
Affected Version(s): * Up to (including) 2019-12-20					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2024	6.1	FlyCms through abbaa5a allows XSS via the permission management feature. **CVE ID : CVE-2024-21732**	N/A	A-FLY-FLYC-290124/87
Vendor: follow-redirects					
Product: follow_redirects					
Affected Version(s): * Up to (excluding) 1.15.4					
URL Redirection to Untrusted Site ('Open Redirect')	02-Jan-2024	6.1	Versions of the package follow-redirects before 1.15.4 are vulnerable to Improper Input Validation due to the improper handling of URLs by the url.parse() function. When new URL() throws an error, it can be manipulated to misinterpret the hostname. An attacker could exploit this weakness to redirect traffic to a malicious site, potentially leading to information disclosure, phishing attacks, or other security breaches. **CVE ID : CVE-2023-26159**	https://github.com/follow-redirects/follow-redirects/pull/236	A-FOL-FOLL-290124/88
Vendor: fooplugins					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: foogallery					
Affected Version(s): * Up to (excluding) 2.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	5.4	The Best WordPress Gallery Plugin – FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom attributes in all versions up to, and including, 2.3.3 due to insufficient input sanitization and output escaping. This makes it possible for contributors and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6747**	N/A	A-FOO-FOOG-290124/89
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 2.1.2					
N/A	03-Jan-2024	7.5	Froxlor is open source server administration software. Prior to version 2.1.2, it was possible to submit the registration form with the essential fields, such as the	https://github.com/Froxlor/Froxlor/commit/4b1846883d4828962add91bd844596d89a9c7cac, https://github.com/Froxlor/Froxlor/security/a	A-FRO-FROX-290124/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			username and password, left intentionally blank. This inadvertent omission allowed for a bypass of the mandatory field requirements (e.g. surname, company name) established by the system. Version 2.1.2 fixes this issue. **CVE ID : CVE-2023-50256**	dvisories/GHSA-625g-fm5w-w7w4	
Vendor: ftpdmin_project					
Product: ftpdmin					
Affected Version(s): 0.96					
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability has been found in Sentex FTPDMIN 0.96 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component RNFR Command Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249817 was assigned to this vulnerability.	N/A	A-FTP-FTPD-290124/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0261		
Vendor: fuwushe					
Product: ifair					
Affected Version(s): * Up to (including) 23.8_ad0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	7.5	Directory Traversal vulnerability in fuwushe.org iFair versions 23.8_ad0 and before allows an attacker to obtain sensitive information via a crafted script. **CVE ID : CVE-2023-47473**	N/A	A-FUW-IFAI-290124/92
Vendor: g5plus					
Product: essential_real_estate					
Affected Version(s): * Up to (excluding) 4.4.0					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	8.8	The Essential Real Estate WordPress plugin before 4.4.0 does not prevent users with limited privileges on the site, like subscribers, from momentarily uploading malicious PHP files disguised as ZIP archives, which may lead to remote code execution. **CVE ID : CVE-2023-6140**	N/A	A-G5P-ESSE-290124/93
N/A	08-Jan-2024	6.5	The Essential Real Estate WordPress plugin before 4.4.0 does not apply	N/A	A-G5P-ESSE-290124/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Denial of Service attacks. **CVE ID : CVE-2023-6139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	The Essential Real Estate WordPress plugin before 4.4.0 does not apply proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Stored XSS attacks. **CVE ID : CVE-2023-6141**	N/A	A-G5P-ESSE-290124/95
Vendor: gecka					
Product: terms_thumbnails					
Affected Version(s): * Up to (including) 1.1					
Deserialization of Untrusted Data	08-Jan-2024	8.8	Deserialization of Untrusted Data vulnerability in Gecka Gecka Terms Thumbnails.This issue affects Gecka Terms Thumbnails: from n/a through 1.1.	N/A	A-GEC-TERM-290124/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52219		
Vendor: geniecompany					
Product: aladdin_connect					
Affected Version(s): * Up to (excluding) 5.73					
Insecure Storage of Sensitive Information	03-Jan-2024	6.8	Users' product account authentication data was stored in clear text in The Genie Company Aladdin Connect Mobile Application Version 5.65 Build 2075 (and below) on Android Devices. This allows the attacker, with access to the android device, to potentially retrieve users' clear text authentication credentials. **CVE ID : CVE-2023-5879**	https://www.rapid7.com/blog/post/2024/01/03/genie-aladdin-connect-retrofit-garage-door-opener-multiple-vulnerabilities/	A-GEN-ALAD-290124/97
Vendor: Get-simple					
Product: getsimplecms					
Affected Version(s): 3.3.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	A Cross Site Scripting (XSS) vulnerability in GetSimple CMS 3.3.16 exists when using Source Code Mode as a backend user to add articles via the	N/A	A-GET-GETS-290124/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/admin/edit.php page. **CVE ID : CVE-2023-51246**		
Vendor: getawesomesupport					
Product: awesome_support					
Affected Version(s): * Up to (including) 6.1.5					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Awesome Support Team Awesome Support – WordPress HelpDesk & Support Plugin.This issue affects Awesome Support – WordPress HelpDesk & Support Plugin: from n/a through 6.1.5. **CVE ID : CVE-2023-51538**	N/A	A-GET-AWES-290124/99
Vendor: gilacms					
Product: gila_cms					
Affected Version(s): * Up to (including) 1.15.4					
Improper Neutralization of Special Elements used in an SQL Command	02-Jan-2024	3.8	SQL Injection vulnerability discovered in Gila CMS 1.15.4 and earlier allows a remote attacker to execute arbitrary web scripts via the Area parameter	https://github.com/GilaCMS/gila/security/policy	A-GIL-GILA-290124/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			under the Administration>Widget tab after the login portal. **CVE ID : CVE-2020-26623**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jan-2024	3.8	A SQL injection vulnerability was discovered in Gila CMS 1.15.4 and earlier which allows a remote attacker to execute arbitrary web scripts via the ID parameter after the login portal. **CVE ID : CVE-2020-26624**	https://github.com/GilaCMS/gila/security/policy	A-GIL-GILA-290124/101
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Jan-2024	3.8	A SQL injection vulnerability was discovered in Gila CMS 1.15.4 and earlier which allows a remote attacker to execute arbitrary web scripts via the 'user_id' parameter after the login portal. **CVE ID : CVE-2020-26625**	https://github.com/GilaCMS/gila/security/policy	A-GIL-GILA-290124/102
Vendor: Github					
Product: cmark-gfm					
Affected Version(s): * Up to (excluding) 0.28.3.gfm.21					
Integer Overflow or Wraparound	04-Jan-2024	9.8	CommonMarker versions prior to 0.23.4 are at risk of an integer overflow vulnerability. This	https://github.com/gjtorikian/commonmarker/commit/ab4504fd17460627a6a	A-GIT-CMAR-290124/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in possibly unauthenticated remote attackers to cause heap memory corruption, potentially leading to an information leak or remote code execution, via parsing tables with marker rows that contain more than UINT16_MAX columns. **CVE ID : CVE-2024-22051**	b255bc3c63e8e5fc6aed3, https://github.com/gjtorikian/commonmarker/security/advisories/GHSA-fmx4-26r3-wxpf	
Affected Version(s): From (including) 0.29.0.gfm.0 Up to (excluding) 0.29.0.gfm.3					
Integer Overflow or Wraparound	04-Jan-2024	9.8	CommonMarker versions prior to 0.23.4 are at risk of an integer overflow vulnerability. This vulnerability can result in possibly unauthenticated remote attackers to cause heap memory corruption, potentially leading to an information leak or remote code execution, via parsing tables with marker rows that contain more than UINT16_MAX columns.	https://github.com/gjtorikian/commonmarker/commit/ab4504fd17460627a6ab255bc3c63e8e5fc6aed3, https://github.com/gjtorikian/commonmarker/security/advisories/GHSA-fmx4-26r3-wxpf	A-GIT-CMAR-290124/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22051		
Vendor: gjtorikian					
Product: commonmarker					
Affected Version(s): * Up to (excluding) 0.23.4					
Integer Overflow or Wraparound	04-Jan-2024	9.8	CommonMarker versions prior to 0.23.4 are at risk of an integer overflow vulnerability. This vulnerability can result in possibly unauthenticated remote attackers to cause heap memory corruption, potentially leading to an information leak or remote code execution, via parsing tables with marker rows that contain more than UINT16_MAX columns. **CVE ID : CVE-2024-22051**	https://github.com/gjtorikian/commonmarker/commit/ab4504fd17460627a6ab255bc3c63e8e5fc6aed3, https://github.com/gjtorikian/commonmarker/security/advisories/GHSA-fmx4-26r3-wxpf	A-GJT-COMM-290124/105
Vendor: GNU					
Product: libredwg					
Affected Version(s): * Up to (excluding) 0.12.5.6384					
Out-of-bounds Read	02-Jan-2024	7.5	Versions of the package libredwg before 0.12.5.6384 are vulnerable to Denial of Service	https://github.com/LibreDWG/libredwg/commit/c8cf03ce4c2315b146caf582e	A-GNU-LIBR-290124/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) due to an out-of-bounds read involving section->num_pages in decode_r2007.c. **CVE ID : CVE-2023-26157**	a061c0460193bcc, https://github.com/LibreDWG/libredwg/issues/850	
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 120.0.6099.199					
Use After Free	04-Jan-2024	8.8	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 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-2024-0222**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html, https://crbug.com/1501798	A-GOO-CHRO-290124/107
Out-of-bounds Write	04-Jan-2024	8.8	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://crbug.com/1505009	A-GOO-CHRO-290124/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0223		
Use After Free	04-Jan-2024	8.8	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0224**	https://crbug.com/1505086	A-GOO-CHRO-290124/109
Use After Free	04-Jan-2024	8.8	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0225**	https://crbug.com/1506923	A-GOO-CHRO-290124/110
Vendor: gov.uk					
Product: govuk_tech_docs					
Affected Version(s): From (including) 2.0.2 Up to (excluding) 3.3.1					
Improper Neutralization of Input During Web Page Generation	04-Jan-2024	6.1	govuk_tech_docs versions from 2.0.2 to before 3.3.1 are vulnerable to a cross-site scripting vulnerability. Malicious	https://github.com/advisories/GHSA-x2xw-hw8g-6773, https://github.com/alphagov/tech-docs-	A-GOV-GOVU-290124/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			JavaScript may be executed in the user's browser if a malicious search result is displayed on the search page. **CVE ID : CVE-2024-22048**	gem/pull/323, https://github.com/alphagov/tech-docs-gem/releases/tag/v3.3.1, https://github.com/alphagov/tech-docs-gem/security/advisories/GHSA-x2xw-hw8g-6773	
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (excluding) 2.3.0					
Out-of-bounds Read	08-Jan-2024	9.1	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV. **CVE ID : CVE-2024-0322**	https://github.com/gpac/gpac/commit/092904b80edbc4dce315684a59cc3184c45c1b70	A-GPA-GPAC-290124/112
Affected Version(s): * Up to (excluding) 2.3.0-dev					
Out-of-bounds Write	08-Jan-2024	9.8	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3-DEV. **CVE ID : CVE-2024-0321**	https://github.com/gpac/gpac/commit/d0ced41651b279bb054eb6390751e2d4eb84819a	A-GPA-GPAC-290124/113
Affected Version(s): 2.3-dev-rev605-gfc9e29089-master					
N/A	03-Jan-2024	7.5	An issue discovered in GPAC 2.3-DEV-rev605-gfc9e29089-master in MP4Box in gf_avc_change_vui /afltest/gpac/src/media_tools/av_parsers.c:6872:55	https://github.com/gpac/gpac/commit/4248def5d24325aeb0e35cacde3d56c9411816a6, https://github.c	A-GPA-GPAC-290124/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to crash the application. **CVE ID : CVE-2023-46929**	om/gpac/gpac/issues/2662	
Affected Version(s): 2.3.0					
Out-of-bounds Read	08-Jan-2024	9.1	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV. **CVE ID : CVE-2024-0322**	https://github.com/gpac/gpac/commit/092904b80edbc4dce315684a59cc3184c45c1b70	A-GPA-GPAC-290124/115
Vendor: gtkwave					
Product: gtkwave					
Affected Version(s): 3.3.115					
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the FST_BL_GEOM parsing maxhandle functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-32650**	N/A	A-GTK-GTKW-290124/116
Improper Restriction of Operations within the	08-Jan-2024	7.8	An improper array index validation vulnerability exists in the EVCD var len parsing	N/A	A-GTK-GTKW-290124/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			functionality of GTKWave 3.3.115. A specially crafted .evcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34087**		
Out-of-bounds Write	08-Jan-2024	7.8	An out-of-bounds write vulnerability exists in the LXT2 num_time_table_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34436**	N/A	A-GTK-GTKW-290124/118
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the VZT longest_len value allocation functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious	N/A	A-GTK-GTKW-290124/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file to trigger this vulnerability. **CVE ID : CVE-2023-35004**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the LXT2 lxt2_rd_trace value elements allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35057**	N/A	A-GTK-GTKW-290124/120
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the fstReaderIterBlocks2 time_table tsec_nitems functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35128**	N/A	A-GTK-GTKW-290124/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the LXT2 zlib block allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35989**	N/A	A-GTK-GTKW-290124/122
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the FST fstReaderIterBlocks2 vesc allocation functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35992**	N/A	A-GTK-GTKW-290124/123
Out-of-bounds Write	08-Jan-2024	7.8	An out-of-bounds write vulnerability exists in the VZT LZMA_read_varint functionality of GTKWave 3.3.115.	N/A	A-GTK-GTKW-290124/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-36861**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	An integer overflow vulnerability exists in the fstReaderIterBlocks2 temp_signal_value_buf allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-36864**	N/A	A-GTK-GTKW-290124/125
Out-of-bounds Write	08-Jan-2024	7.8	An out-of-bounds write vulnerability exists in the VZT LZMA_Read dmem extraction functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious	N/A	A-GTK-GTKW-290124/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file to trigger this vulnerability. **CVE ID : CVE-2023-37282**		
Out-of-bounds Write	08-Jan-2024	7.8	A stack-based buffer overflow vulnerability exists in the LXT2 lxt2_rd_expand_integer_to_bits function of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38583**	N/A	A-GTK-GTKW-290124/127
Out-of-bounds Write	08-Jan-2024	7.8	An out-of-bounds write vulnerability exists in the LXT2 zlib block decompression functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38657**	N/A	A-GTK-GTKW-290124/128
Vendor: hamidrezasepehr					
Product: wp_custom_cursors_|_wordpress_cursor_plugin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	4.8	The WP Custom Cursors | WordPress Cursor Plugin WordPress plugin through 3.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-5911**	N/A	A-HAM-WP_C-290124/129
Vendor: hayyp					
Product: cherry					
Affected Version(s): * Up to (including) 2021-01-05					
Out-of-bounds Write	05-Jan-2024	9.8	handle_request in http.c in cherry through 4b877df has an sscanf stack-based buffer overflow via a long URI, leading to remote code execution. **CVE ID : CVE-2024-22086**	N/A	A-HAY-CHER-290124/130
Vendor: hcltech					
Product: dryice_myxalytics					
Affected Version(s): 5.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal arbitrary file read vulnerability because it uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. The product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Potential exploits can completely disrupt or take over the application. **CVE ID : CVE-2023-45722**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/131
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal vulnerability which allows file upload capability. Certain endpoints permit users to	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate the path (including the file name) where these files are stored on the server. **CVE ID : CVE-2023-45723**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	9.8	HCL DRYiCE MyXalytics product is impacted by unauthenticated file upload vulnerability. The web application permits the upload of a certain file without requiring user authentication. **CVE ID : CVE-2023-45724**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/133
N/A	03-Jan-2024	9.1	HCL DRYiCE MyXalytics is impacted by the use of an insecure key rotation mechanism which can allow an attacker to compromise the confidentiality or integrity of data. **CVE ID : CVE-2023-50351**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/134
Use of a Broken or Risky Cryptographic Algorithm	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by the use of a broken cryptographic algorithm for encryption,	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially giving an attacker ability to decrypt sensitive information. **CVE ID : CVE-2023-50350**		
N/A	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by Improper Access Control (Obsolete web pages) vulnerability. Discovery of outdated and accessible web pages, reflects a "Missing Access Control" vulnerability, which could lead to inadvertent exposure of sensitive information and/or exposing a vulnerable endpoint. **CVE ID : CVE-2023-50341**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/136
N/A	03-Jan-2024	6.5	HCL DRYiCE MyXalytics is impacted by an Improper Access Control (Controller APIs) vulnerability. Certain API endpoints are accessible to Customer Admin Users that can allow access to	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information about other users. **CVE ID : CVE-2023-50343**		
URL Redirection to Untrusted Site ('Open Redirect')	03-Jan-2024	6.1	HCL DRYiCE MyXalytics is impacted by an Open Redirect vulnerability which could allow an attacker to redirect users to malicious sites, potentially leading to phishing attacks or other security threats. **CVE ID : CVE-2023-50345**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/138
N/A	03-Jan-2024	5.4	HCL DRYiCE MyXalytics is impacted by improper access control (Unauthenticated File Download) vulnerability. An unauthenticated user can download certain files. **CVE ID : CVE-2023-50344**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/139
N/A	03-Jan-2024	5.3	HCL DRYiCE MyXalytics is impacted by an improper error handling vulnerability. The application returns detailed error messages that can	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide an attacker with insight into the application, system, etc. **CVE ID : CVE-2023-50348**		
N/A	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an information disclosure vulnerability. Certain endpoints within the application disclose detailed file information. **CVE ID : CVE-2023-50346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/141
Authorization Bypass Through User-Controlled Key	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an Insecure Direct Object Reference (IDOR) vulnerability. A user can obtain certain details about another user as a result of improper access control. **CVE ID : CVE-2023-50342**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/142
Affected Version(s): 6.0					
Improper Limitation of a Pathname to a Restricted Directory	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal arbitrary file read vulnerability because it uses	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. The product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Potential exploits can completely disrupt or take over the application. **CVE ID : CVE-2023-45722**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal vulnerability which allows file upload capability. Certain endpoints permit users to manipulate the path (including the file name) where these files are stored on the server.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45723		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	9.8	HCL DRYiCE MyXalytics product is impacted by unauthenticated file upload vulnerability. The web application permits the upload of a certain file without requiring user authentication. **CVE ID : CVE-2023-45724**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/145
N/A	03-Jan-2024	9.1	HCL DRYiCE MyXalytics is impacted by the use of an insecure key rotation mechanism which can allow an attacker to compromise the confidentiality or integrity of data. **CVE ID : CVE-2023-50351**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/146
Use of a Broken or Risky Cryptographic Algorithm	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by the use of a broken cryptographic algorithm for encryption, potentially giving an attacker ability to decrypt sensitive information.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50350		
N/A	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by Improper Access Control (Obsolete web pages) vulnerability. Discovery of outdated and accessible web pages, reflects a "Missing Access Control" vulnerability, which could lead to inadvertent exposure of sensitive information and/or exposing a vulnerable endpoint. **CVE ID : CVE-2023-50341**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/148
N/A	03-Jan-2024	6.5	HCL DRYiCE MyXalytics is impacted by an Improper Access Control (Controller APIs) vulnerability. Certain API endpoints are accessible to Customer Admin Users that can allow access to sensitive information about other users.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50343		
URL Redirection to Untrusted Site ('Open Redirect')	03-Jan-2024	6.1	HCL DRYiCE MyXalytics is impacted by an Open Redirect vulnerability which could allow an attacker to redirect users to malicious sites, potentially leading to phishing attacks or other security threats. **CVE ID : CVE-2023-50345**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/150
N/A	03-Jan-2024	5.4	HCL DRYiCE MyXalytics is impacted by improper access control (Unauthenticated File Download) vulnerability. An unauthenticated user can download certain files. **CVE ID : CVE-2023-50344**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/151
N/A	03-Jan-2024	5.3	HCL DRYiCE MyXalytics is impacted by an improper error handling vulnerability. The application returns detailed error messages that can provide an attacker with insight into the application, system, etc.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50348		
N/A	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an information disclosure vulnerability. Certain endpoints within the application disclose detailed file information. **CVE ID : CVE-2023-50346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/153
Authorization Bypass Through User-Controlled Key	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an Insecure Direct Object Reference (IDOR) vulnerability. A user can obtain certain details about another user as a result of improper access control. **CVE ID : CVE-2023-50342**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/154
Affected Version(s): 6.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal arbitrary file read vulnerability because it uses external input to construct a pathname that is intended to	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identify a file or directory that is located underneath a restricted parent directory. The product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Potential exploits can completely disrupt or take over the application. **CVE ID : CVE-2023-45722**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	9.8	HCL DRYiCE MyXalytics is impacted by path traversal vulnerability which allows file upload capability. Certain endpoints permit users to manipulate the path (including the file name) where these files are stored on the server. **CVE ID : CVE-2023-45723**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/156
Unrestricted Upload of File with	03-Jan-2024	9.8	HCL DRYiCE MyXalytics product is impacted by	https://support.hcltechsw.com/csm?id=kb_artic	A-HCL-DRYI-290124/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			unauthenticated file upload vulnerability. The web application permits the upload of a certain file without requiring user authentication. **CVE ID : CVE-2023-45724**	le&sysparm_article=KB0109608	
N/A	03-Jan-2024	9.1	HCL DRYiCE MyXalytics is impacted by the use of an insecure key rotation mechanism which can allow an attacker to compromise the confidentiality or integrity of data. **CVE ID : CVE-2023-50351**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/158
Use of a Broken or Risky Cryptographic Algorithm	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by the use of a broken cryptographic algorithm for encryption, potentially giving an attacker ability to decrypt sensitive information. **CVE ID : CVE-2023-50350**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Jan-2024	7.5	HCL DRYiCE MyXalytics is impacted by Improper Access Control (Obsolete web pages) vulnerability. Discovery of outdated and accessible web pages, reflects a "Missing Access Control" vulnerability, which could lead to inadvertent exposure of sensitive information and/or exposing a vulnerable endpoint. **CVE ID : CVE-2023-50341**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/160
N/A	03-Jan-2024	6.5	HCL DRYiCE MyXalytics is impacted by an Improper Access Control (Controller APIs) vulnerability. Certain API endpoints are accessible to Customer Admin Users that can allow access to sensitive information about other users.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50343		
URL Redirection to Untrusted Site ('Open Redirect')	03-Jan-2024	6.1	HCL DRYiCE MyXalytics is impacted by an Open Redirect vulnerability which could allow an attacker to redirect users to malicious sites, potentially leading to phishing attacks or other security threats. **CVE ID : CVE-2023-50345**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/162
N/A	03-Jan-2024	5.4	HCL DRYiCE MyXalytics is impacted by improper access control (Unauthenticated File Download) vulnerability. An unauthenticated user can download certain files. **CVE ID : CVE-2023-50344**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/163
N/A	03-Jan-2024	5.3	HCL DRYiCE MyXalytics is impacted by an improper error handling vulnerability. The application returns detailed error messages that can provide an attacker with insight into	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the application, system, etc. **CVE ID : CVE-2023-50348**		
N/A	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an information disclosure vulnerability. Certain endpoints within the application disclose detailed file information. **CVE ID : CVE-2023-50346**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/165
Authorization Bypass Through User-Controlled Key	03-Jan-2024	4.3	HCL DRYiCE MyXalytics is impacted by an Insecure Direct Object Reference (IDOR) vulnerability. A user can obtain certain details about another user as a result of improper access control. **CVE ID : CVE-2023-50342**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109608	A-HCL-DRYI-290124/166
Vendor: huiran_host_reseller_system_project					
Product: huiran_host_reseller_system					
Affected Version(s): * Up to (including) 2.0.0					
Weak Password	02-Jan-2024	8.1	A vulnerability classified as	N/A	A-HUI-HUIR-290124/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Recovery Mechanism for Forgotten Password			problematic has been found in HuiRan Host Reseller System up to 2.0.0. Affected is an unknown function of the file /user/index/findpass?do=4 of the component HTTP POST Request Handler. The manipulation leads to weak password recovery. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249444. **CVE ID : CVE-2024-0186**		
Vendor: i13websolution					
Product: email_subscription_popup					
Affected Version(s): * Up to (excluding) 1.2.20					
Improper Neutralization of Input During Web Page Generation	08-Jan-2024	6.1	The Email Subscription Popup WordPress plugin before 1.2.20 does not sanitise and escape a parameter before	N/A	A-I13-EMAI-290124/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-2023-6555**		
Vendor: IBM					
Product: cics_transaction_gateway					
Affected Version(s): 9.3					
N/A	08-Jan-2024	8.1	IBM CICS Transaction Gateway 9.3 could allow a user to transfer or view files due to improper access controls. IBM X-Force ID: 270259. **CVE ID : CVE-2023-47140**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270259, https://www.ibm.com/support/pages/node/7105094	A-IBM-CICS-290124/169
Product: db2					
Affected Version(s): From (including) 10.5 Up to (excluding) 10.5.0.11					
N/A	07-Jan-2024	7.8	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402.	https://exchange.xforce.ibmcloud.com/vulnerabilities/270402, https://www.ibm.com/support/pages/node/7105500	A-IBM-DB2-290124/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47145		
Affected Version(s): From (including) 11.1 Up to (excluding) 11.1.4.7					
N/A	07-Jan-2024	7.8	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402. **CVE ID : CVE-2023-47145**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270402, https://www.ibm.com/support/pages/node/7105500	A-IBM-DB2-290124/171
Affected Version(s): From (including) 11.5 Up to (excluding) 11.5.8					
N/A	07-Jan-2024	7.8	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402. **CVE ID : CVE-2023-47145**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270402, https://www.ibm.com/support/pages/node/7105500	A-IBM-DB2-290124/172
Product: storage_fusion_hci					
Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.7.1					
Use of Hard-coded Credentials	08-Jan-2024	9.8	IBM Storage Fusion HCI 2.1.0 through 2.6.1 contains hard-coded credentials, such as	https://exchange.xforce.ibmcloud.com/vulnerabilities/275671, https://www.ib	A-IBM-STOR-290124/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 275671. **CVE ID : CVE-2023-50948**	m.com/support/pages/node/7105509	
Vendor: icegram					
Product: icegram_engage					
Affected Version(s): * Up to (including) 3.1.18					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Icegram Icegram Engage – WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building.This issue affects Icegram Engage – WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building: from n/a through 3.1.18. **CVE ID : CVE-2023-52119**	N/A	A-ICE-ICEG-290124/174
Vendor: Icewarp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: icewarp					
Affected Version(s): 12.0.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	6.1	A vulnerability classified as problematic has been found in IceWarp 12.0.2.1/12.0.3.1. This affects an unknown part of the file /install/ of the component Utility Download Handler. The manipulation of the argument lang with the input 1%27"()%26%25<zzz><ScRiPt>alert(document.domain)</ScRiPt> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249759. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0246**	N/A	A-ICE-ICEW-290124/175
Affected Version(s): 12.0.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	6.1	A vulnerability classified as problematic has been found in IceWarp 12.0.2.1/12.0.3.1. This affects an unknown part of the file /install/ of the component Utility Download Handler. The manipulation of the argument lang with the input 1%27"()%26%25<zzz><ScRiPt>alert(document.domain)</ScRiPt> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249759. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0246**	N/A	A-ICE-ICEW-290124/176
Vendor: ideabox					
Product: powerpack_addons_for_elementor					
Affected Version(s): * Up to (excluding) 2.7.14					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	03-Jan-2024	4.3	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.13. This is due to missing or incorrect nonce validation in the powerpack-lite-for-elementor/classes/class-pp-admin-settings.php file. This makes it possible for unauthenticated attackers to modify and reset plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-6984**	https://www.wordfence.com/threat-intel/vulnerabilities/id/fe2cfc96-63f4-4e4b-bf49-6031594a4805?source=cve	A-IDE-POWE-290124/177
Vendor: iframe_project					
Product: iframe					
Affected Version(s): * Up to (including) 4.8					
Improper Neutralization of Input	05-Jan-2024	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-IFR-IFRA-290124/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			('Cross-site Scripting') vulnerability in webvitaly iframe allows Stored XSS.This issue affects iframe: from n/a through 4.8. **CVE ID : CVE-2023-52125**		
Vendor: impactpixel					
Product: ads_invalid_click_protection					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Impactpixel Ads Invalid Click Protection allows Stored XSS.This issue affects Ads Invalid Click Protection: from n/a through 1.0. **CVE ID : CVE-2023-52197**	N/A	A-IMP-ADS_-290124/179
Vendor: inis_project					
Product: inis					
Affected Version(s): * Up to (including) 2.0.1					
Server-Side	08-Jan-2024	8.8	A vulnerability was found in Inis up to	N/A	A-INI-INIS-290124/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			2.0.1. It has been rated as critical. This issue affects some unknown processing of the file app/api/controller/default/Proxy.php. The manipulation of the argument p_url leads to server-side request forgery. 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-249875. **CVE ID : CVE-2024-0308**		
Vendor: Irfanview					
Product: b3d					
Affected Version(s): * Up to (excluding) 4.56					
Out-of-bounds Write	05-Jan-2024	9.8	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+27ef heap-based out-of-bounds write. **CVE ID : CVE-2020-13878**	N/A	A-IRF-B3D-290124/181
Out-of-bounds Write	05-Jan-2024	9.8	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+214f	N/A	A-IRF-B3D-290124/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap-based out-of-bounds write. **CVE ID : CVE-2020-13879**		
Out-of-bounds Write	05-Jan-2024	9.8	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+1cbf heap-based out-of-bounds write. **CVE ID : CVE-2020-13880**	N/A	A-IRF-B3D-290124/183
Vendor: ivanti					
Product: connect_secure					
Affected Version(s): 22.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/184
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-	A-IVA-CONN-290124/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	
Affected Version(s): 22.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/186
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-	A-IVA-CONN-290124/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				Gateways?language=en_US	
Affected Version(s): 22.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/188
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/189
Affected Version(s): 22.4					
Improper Neutralization of Special	12-Jan-2024	9.1	A command injection vulnerability in web components of	https://forums.ivanti.com/s/article/CVE-2023-46805-	A-IVA-CONN-290124/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/191
Affected Version(s): 22.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-	A-IVA-CONN-290124/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	Secure-Gateways?language=en_US	
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/193
Affected Version(s): 22.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/195
Affected Version(s): 9.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/196
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-	A-IVA-CONN-290124/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	
Affected Version(s): 9.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/198
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-CONN-290124/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 2022					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jan-2024	8.8	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server. **CVE ID : CVE-2023-39336**	https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US	A-IVA-ENDP-290124/200
Affected Version(s): 2022					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jan-2024	8.8	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to	https://forums.ivanti.com/s/article/SA-2023-12-19-CVE-2023-39336?language=en_US	A-IVA-ENDP-290124/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCE on the core server. **CVE ID : CVE-2023-39336**		
Product: policy_secure					
Affected Version(s): 22.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/202
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/203
Affected Version(s): 22.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/204
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/205
Affected Version(s): 22.3					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x)	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-	A-IVA-POLI-290124/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/207
Affected Version(s): 22.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the appliance. **CVE ID : CVE-2024-21887**		
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/209
Affected Version(s): 22.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/210
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the	https://forums.ivanti.com/s/article/CVE-2023-	A-IVA-POLI-290124/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	
Affected Version(s): 22.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/212
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-	A-IVA-POLI-290124/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing control checks. **CVE ID : CVE-2023-46805**	Ivanti-Policy-Secure-Gateways?language=en_US	
Affected Version(s): 9.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/214
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/215
Affected Version(s): 9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Jan-2024	9.1	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. **CVE ID : CVE-2024-21887**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/216
Improper Authentication	12-Jan-2024	8.2	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks. **CVE ID : CVE-2023-46805**	https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	A-IVA-POLI-290124/217
Vendor: janobe					
Product: engineers_online_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	01-Jan-2024	9.8	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and	N/A	A-JAN-ENGI-290124/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			classified as critical. Affected by this issue is some unknown functionality of the file /admin/ of the component Admin Login. The manipulation of the argument username/password leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-249440. **CVE ID : CVE-2024-0182**		
Vendor: javik					
Product: randomize					
Affected Version(s): * Up to (including) 1.4.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Javik Randomize.This issue affects Randomize: from n/a through 1.4.3. **CVE ID : CVE-2023-52204**	N/A	A-JAV-RAND-290124/219
Vendor: jeecg					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jeecg					
Affected Version(s): * Up to (including) 4.0					
Deserialization of Untrusted Data	03-Jan-2024	9.8	Deserialization of Untrusted Data in jeecgFormDemoController in JEECG 4.0 and earlier allows attackers to run arbitrary code via crafted POST request. **CVE ID : CVE-2023-49442**	N/A	A-JEE-JEEC-290124/220
Vendor: Jetbrains					
Product: youtrack					
Affected Version(s): * Up to (excluding) 2023.3.22666					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	In JetBrains YouTrack before 2023.3.22666 stored XSS via markdown was possible **CVE ID : CVE-2024-22370**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-YOUT-290124/221
Vendor: jizhicms					
Product: jizhicms					
Affected Version(s): 2.5.0					
N/A	04-Jan-2024	9.8	Jizhicms v2.5 was discovered to contain an arbitrary file download vulnerability via the component /admin/c/PluginsController.php. **CVE ID : CVE-2023-51154**	N/A	A-JIZ-JIZH-290124/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: john_nunemaker					
Product: httparty					
Affected Version(s): * Up to (excluding) 0.21.0					
Exposure of Resource to Wrong Sphere	04-Jan-2024	5.3	httparty before 0.21.0 is vulnerable to an assumed-immutable web parameter vulnerability. A remote and unauthenticated attacker can provide a crafted filename parameter during multipart/form-data uploads which could result in attacker controlled filenames being written. **CVE ID : CVE-2024-22049**	https://github.com/jnunemaker/httparty/commit/cdb45a678c43e44570b4e73f84b1abeb5ec22b8e, https://github.com/jnunemaker/httparty/security/advisories/GHSA-5pq7-52mg-hr42, https://vulncheck.com/advisories/vc-advisory-GHSA-5pq7-52mg-hr42	A-JOH-HTTP-290124/223
Vendor: juzaweb					
Product: cms					
Affected Version(s): * Up to (including) 3.4					
N/A	09-Jan-2024	4.9	juzaweb <= 3.4 is vulnerable to Incorrect Access Control, resulting in an application outage after a 500 HTTP status code. The payload in the timezone field was not correctly validated.	N/A	A-JUZ-CMS-290124/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46906		
Vendor: kashipara					
Product: billing_software					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'itemnameid' parameter of the material_bill.php?action=itemRelation resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49622**	N/A	A-KAS-BILL-290124/225
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'cancelid' parameter of the material_bill.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-BILL-290124/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49624		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the partylist_edit_submit.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49625**	N/A	A-KAS-BILL-290124/227
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'buyer_address' parameter of the buyer_detail_submit.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49633**	N/A	A-KAS-BILL-290124/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'customer_details' parameter of the buyer_invoice_submit.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49639**	N/A	A-KAS-BILL-290124/229
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'bank_details' parameter of the party_submit.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49658**	N/A	A-KAS-BILL-290124/230
Improper Neutralization of	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple	N/A	A-KAS-BILL-290124/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Unauthenticated SQL Injection vulnerabilities. The 'quantity[]' parameter of the submit_delivery_list.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49665**		
Product: billing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'custmer_details' parameter of the submit_material_list.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49666**	N/A	A-KAS-BILL-290124/232
Product: food_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	9.8	A vulnerability was found in Kashipara Food Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file itemBillPdf.php. The manipulation of the argument printid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249848. **CVE ID : CVE-2024-0287**	N/A	A-KAS-FOOD-290124/233
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	9.8	A vulnerability classified as critical has been found in Kashipara Food Management System 1.0. This affects an unknown part of the file rawstock_used_damaged_submit.php. The manipulation of the argument product_name leads to sql injection. It is possible to initiate the attack	N/A	A-KAS-FOOD-290124/234

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 VDB-249849 was assigned to this vulnerability. **CVE ID : CVE-2024-0288**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	9.8	A vulnerability classified as critical was found in Kashipara Food Management System 1.0. This vulnerability affects unknown code of the file stock_entry_submit.php. The manipulation of the argument itemype leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249850 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0289**	https://github.com/laoquanshi/heishou/blob/main/Food Management System SQL Injection Vulnerability14.md	A-KAS-FOOD-290124/235
Improper Neutralization of Special Elements used in an	08-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Kashipara Food Management	N/A	A-KAS-FOOD-290124/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			System 1.0. This issue affects some unknown processing of the file stock_edit.php. The manipulation of the argument item_type 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-249851. **CVE ID : CVE-2024-0290**		
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file item_list_submit.php. The manipulation of the argument item_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-KAS-FOOD-290124/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier VDB-249825 was assigned to this vulnerability. **CVE ID : CVE-2024-0270**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file addmaterial_edit.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249826 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0271**	N/A	A-KAS-FOOD-290124/238
Improper Neutralization of Special Elements used in an SQL Command	07-Jan-2024	6.5	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. This issue affects some unknown processing of the	N/A	A-KAS-FOOD-290124/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			file addmaterialsubmit.php. The manipulation of the argument material_name 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-249827. **CVE ID : CVE-2024-0272**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as critical. Affected is an unknown function of the file addwaste_entry.php. The manipulation of the argument item_name 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-249828.	N/A	A-KAS-FOOD-290124/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0273		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file billAjax.php. The manipulation of the argument item_name 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-249829 was assigned to this vulnerability. **CVE ID : CVE-2024-0274**	N/A	A-KAS-FOOD-290124/241
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file item_edit_submit.php. The manipulation of the argument id leads	N/A	A-KAS-FOOD-290124/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249830 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0275**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability classified as critical has been found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file rawstock_used_damaged_smt.php. The manipulation of the argument product_name 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-249831. **CVE ID : CVE-2024-0276**	N/A	A-KAS-FOOD-290124/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability classified as critical was found in Kashipara Food Management System up to 1.0. This vulnerability affects unknown code of the file party_submit.php. The manipulation of the argument party_name 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-249832. **CVE ID : CVE-2024-0277**	N/A	A-KAS-FOOD-290124/244
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability, which was classified as critical, has been found in Kashipara Food Management System up to 1.0. This issue affects some unknown processing of the file partylist_edit_submit.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely.	N/A	A-KAS-FOOD-290124/245

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-249833 was assigned to this vulnerability. **CVE ID : CVE-2024-0278**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. Affected is an unknown function of the file item_list_edit.php. 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-249834 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0279**	N/A	A-KAS-FOOD-290124/246
Improper Neutralization of Special Elements used in an	07-Jan-2024	6.5	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as	N/A	A-KAS-FOOD-290124/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			critical. Affected by this vulnerability is an unknown functionality of the file item_type_submit.php. The manipulation of the argument type_name 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-249835. **CVE ID : CVE-2024-0280**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	6.5	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file loginCheck.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-KAS-FOOD-290124/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-249836. **CVE ID : CVE-2024-0281**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	6.1	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as problematic. This affects an unknown part of the file addmaterialsubmit.php. The manipulation of the argument tin 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-249837 was assigned to this vulnerability. **CVE ID : CVE-2024-0282**	N/A	A-KAS-FOOD-290124/249
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	6.1	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file party_details.php. The manipulation	N/A	A-KAS-FOOD-290124/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument party_name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249838 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0283**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	6.1	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as problematic. This issue affects some unknown processing of the file party_submit.php. The manipulation of the argument party_address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249839.	N/A	A-KAS-FOOD-290124/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0284		
Product: online_notice_board_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'dd' parameter of the registration.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50743**	N/A	A-KAS-ONLI-290124/252
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'e' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-ONLI-290124/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50752		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'dd' parameter of the user/update_profile.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50753**	N/A	A-KAS-ONLI-290124/254
Unrestricted Upload of File with Dangerous Type	04-Jan-2024	8.8	Online Notice Board System v1.0 is vulnerable to an Insecure File Upload vulnerability on the 'f' parameter of user/update_profile_pic.php page, allowing an authenticated attacker to obtain Remote Code Execution on the server hosting the application.	N/A	A-KAS-ONLI-290124/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50760		
Product: travel_website					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelIDHidden' parameter of the booking.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50862**	N/A	A-KAS-TRAV-290124/256
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelIDHidden' parameter of the generateReceipt.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-TRAV-290124/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50863		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelId' parameter of the hotelDetails.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50864**	N/A	A-KAS-TRAV-290124/258
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'city' parameter of the hotelSearch.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50865**	N/A	A-KAS-TRAV-290124/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the loginAction.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50866**	N/A	A-KAS-TRAV-290124/260
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Jan-2024	9.8	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the signupAction.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-50867**	N/A	A-KAS-TRAV-290124/261
Vendor: kernelsu					
Product: kernelsu					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 0.7.1					
Authentication Bypass by Spoofing	02-Jan-2024	7.8	KernelSU is a Kernel-based root solution for Android devices. In versions 0.7.1 and prior, the logic of get apk path in KernelSU kernel module can be bypassed, which causes any malicious apk named `me.weishu.kernelsu` get root permission. If a KernelSU module installed device try to install any not checked apk which package name equal to the official KernelSU Manager, it can take over root privileges on the device. As of time of publication, a patched version is not available. **CVE ID : CVE-2023-49794**	https://github.com/tiann/KernelSU/security/advisories/GHSA-8rc5-x54x-5qc4	A-KER-KERN-290124/262
Vendor: kutethemes					
Product: ovic_responsive_wpbakery					
Affected Version(s): * Up to (excluding) 1.2.9					
Deserialization of Untrusted Data	08-Jan-2024	8.8	The Ovic Responsive WPBakery WordPress plugin before 1.2.9 does not limit which options can be	N/A	A-KUT-OVIC-290124/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updated via some of its AJAX actions, which may allow attackers with a subscriber+ account to update blog options, such as 'users_can_register' and 'default_role'. It also unserializes user input in the process, which may lead to Object Injection attacks. **CVE ID : CVE-2023-5235**		
Vendor: laf					
Product: laf					
Affected Version(s): 0.1.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace	N/A	A-LAF-LAF-290124/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.4.1					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/266
Affected Version(s): 0.4.10					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.11					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.12					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.13					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.4.14					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/271
Affected Version(s): 0.4.15					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.16					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.17					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.18					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.4.19					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/276
Affected Version(s): 0.4.2					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.20					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.21					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.3					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.4.4					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/281
Affected Version(s): 0.4.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.6					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.7					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.4.8					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.4.9					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/286
Affected Version(s): 0.5.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.1					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.2					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.3					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.5.4					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/291
Affected Version(s): 0.5.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.6					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.7					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.5.8					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.6.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/296
Affected Version(s): 0.6.1					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.10					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.11					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.12					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.6.13					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/301
Affected Version(s): 0.6.14					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.15					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.16					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.17					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.6.18					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/306
Affected Version(s): 0.6.19					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.2					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.20					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.21					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.6.22					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/311
Affected Version(s): 0.6.23					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.3					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.4					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.6.6					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/316
Affected Version(s): 0.6.7					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.8					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.6.9					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.7.1					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/321
Affected Version(s): 0.7.10					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.11					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.2					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.3					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.7.4					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/326
Affected Version(s): 0.7.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.6					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.7					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.7.8					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.7.9					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/331
Affected Version(s): 0.8.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.1					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.10					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.11					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.8.12					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/336
Affected Version(s): 0.8.13					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.2					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.3					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.4					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 0.8.5					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/341
Affected Version(s): 0.8.6					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses	N/A	A-LAF-LAF-290124/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.7					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior,	N/A	A-LAF-LAF-290124/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.8					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this	N/A	A-LAF-LAF-290124/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**		
Affected Version(s): 0.8.9					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	N/A	A-LAF-LAF-290124/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50253		
Affected Version(s): 1.0.0					
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist. **CVE ID : CVE-2023-50253**	N/A	A-LAF-LAF-290124/346
Vendor: laybuy					
Product: laybuy_payment_extension_for_woocommerce					
Affected Version(s): * Up to (including) 5.3.9					
Improper Neutralization of	08-Jan-2024	5.4	Improper Neutralization of Input During Web	N/A	A-LAY-LAYB-290124/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Page Generation ('Cross-site Scripting') vulnerability in Laybuy Laybuy Payment Extension for WooCommerce allows Stored XSS.This issue affects Laybuy Payment Extension for WooCommerce: from n/a through 5.3.9. **CVE ID : CVE-2024-21745**		
Vendor: Lenovo					
Product: browser_hd					
Affected Version(s): * Up to (excluding) 2.1.4.1					
N/A	03-Jan-2024	7.5	A vulnerability was reported in the Lenovo Browser Mobile and Lenovo Browser HD Apps for Android that could allow an attacker to craft a payload that could result in the disclosure of sensitive information. **CVE ID : CVE-2023-6540**	https://iknow.lenovo.com.cn/detail/419251	A-LEN-BROW-290124/348
Product: browser_mobile					
Affected Version(s): * Up to (excluding) 9.1.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Jan-2024	7.5	A vulnerability was reported in the Lenovo Browser Mobile and Lenovo Browser HD Apps for Android that could allow an attacker to craft a payload that could result in the disclosure of sensitive information. **CVE ID : CVE-2023-6540**	https://iknow.lenovo.com.cn/detail/419251	A-LEN-BROW-290124/349
Product: universal_device_client					
Affected Version(s): * Up to (excluding) 23.10					
Uncontrolled Search Path Element	03-Jan-2024	7.8	Uncontrolled search path vulnerabilities were reported in the Lenovo Universal Device Client (UDC) that could allow an attacker with local access to execute code with elevated privileges. **CVE ID : CVE-2023-6338**	https://support.lenovo.com/us/en/product_security/LEN-121183	A-LEN-UNIV-290124/350
Vendor: Libssh					
Product: libssh					
Affected Version(s): From (including) 0.10.0 Up to (excluding) 0.10.6					
Improper Neutralization of Special Elements in Output Used by a	03-Jan-2024	7.8	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked	https://access.redhat.com/security/cve/CVE-2023-6004, https://lists.fedoraproject.org/archives/list/pa	A-LIB-LIBS-290124/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter. **CVE ID : CVE-2023-6004**	ckage-announce@lists.fedoraproject.org/message/LZQVUHWVWRH73YBXUQJOD6CKHDQBU3DM/	
Affected Version(s): From (including) 0.8.0 Up to (excluding) 0.9.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	7.8	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter. **CVE ID : CVE-2023-6004**	https://access.redhat.com/security/cve/CVE-2023-6004, https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LZQVUHWVWRH73YBXUQJOD6CKHDQBU3DM/	A-LIB-LIBS-290124/352
Vendor: Linecorp					
Product: line					
Affected Version(s): 13.6.1					
N/A	03-Jan-2024	8.2	An issue in Tamaki_hamanoki Line v.13.6.1 allows attackers to send crafted notifications via	N/A	A-LIN-LINE-290124/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leakage of the channel access token. **CVE ID : CVE-2023-45559**		
N/A	02-Jan-2024	5.3	An issue in A-WORLD OIRASE BEER_waiting Line v.13.6.1 allows attackers to send crafted notifications via leakage of the channel access token. **CVE ID : CVE-2023-45561**	N/A	A-LIN-LINE-290124/354
Vendor: linksoftwarellc					
Product: white_label					
Affected Version(s): * Up to (including) 2.9.0					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WhiteWP White Label – WordPress Custom Admin, Custom Login Page, and Custom Dashboard.This issue affects White Label – WordPress Custom Admin, Custom Login Page, and Custom Dashboard: from n/a through 2.9.0. **CVE ID : CVE-2023-52128**	N/A	A-LIN-WHIT-290124/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Linuxfoundation					
Product: backstage					
Affected Version(s): * Up to (excluding) 1.21.0					
Generation of Error Message Containing Sensitive Information	04-Jan-2024	5.7	A flaw was found in the Red Hat Developer Hub (RHDH). The catalog-import function leaks GitLab access tokens on the frontend when the base64 encoded GitLab token includes a newline at the end of the string. The sanitized error can display on the frontend, including the raw access token. Upon gaining access to this token and depending on permissions, an attacker could push malicious code to repositories, delete resources in Git, revoke or generate new keys, and sign code illegitimately. **CVE ID : CVE-2023-6944**	https://access.redhat.com/security/cve/CVE-2023-6944, https://bugzilla.redhat.com/show_bug.cgi?id=2255204	A-LIN-BACK-290124/356
Product: cubefs					
Affected Version(s): * Up to (excluding) 3.3.1					
Use of Insufficient	03-Jan-2024	9.8	CubeFS is an open-source cloud-native file storage system. Prior to	https://github.com/cubefs/cubefs/commit/8555c6402794cab	A-LIN-CUBE-290124/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			version 3.3.1, CubeFS used an insecure random string generator to generate user-specific, sensitive keys used to authenticate users in a CubeFS deployment. This could allow an attacker to predict and/or guess the generated string and impersonate a user thereby obtaining higher privileges. When CubeFS creates new users, it creates a piece of sensitive information for the user called the “accessKey”. To create the "accesKey", CubeFS uses an insecure string generator which makes it easy to guess and thereby impersonate the created user. An attacker could leverage the predictable random string generator and guess a users access key and impersonate the user to obtain higher privileges.	df2cc025c8bea1576122c07ba	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The issue has been fixed in v3.3.1. There is no other mitigation than to upgrade. **CVE ID : CVE-2023-46740**		
N/A	03-Jan-2024	9.8	CubeFS is an open-source cloud-native file storage system. A vulnerability was found in CubeFS prior to version 3.3.1 that could allow users to read sensitive data from the logs which could allow them escalate privileges. CubeFS leaks configuration keys in plaintext format in the logs. These keys could allow anyone to carry out operations on blobs that they otherwise do not have permissions for. For example, an attacker that has succesfully retrieved a secret key from the logs can delete blogs from the blob store. The attacker can either be an internal user with limited privileges to read the log, or they can be an	https://github.com/cubefs/cubefs/commit/972f0275ee8d5dbba4b1530da7c145c269b31ef5	A-LIN-CUBE-290124/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			external user who has escalated privileges sufficiently to access the logs. The vulnerability has been patched in v3.3.1. There is no other mitigation than upgrading. **CVE ID : CVE-2023-46741**		
Allocation of Resources Without Limits or Throttling	03-Jan-2024	6.5	CubeFS is an open-source cloud-native file storage system. A security vulnerability was found in CubeFS HandlerNode in versions prior to 3.3.1 that could allow authenticated users to send maliciously-crafted requests that would crash the ObjectNode and deny other users from using it. The root cause was improper handling of incoming HTTP requests that could allow an attacker to control the ammount of memory that the ObjectNode would allocate. A malicious request could make the	https://github.com/cubefs/cubefs/commit/dd46c24873c8f3df48d0a598b704ef9bd24b1ec1	A-LIN-CUBE-290124/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ObjectNode allocate more memory that the machine had available, and the attacker could exhaust memory by way of a single malicious request. An attacker would need to be authenticated in order to invoke the vulnerable code with their malicious request and have permissions to delete objects. In addition, the attacker would need to know the names of existing buckets of the CubeFS deployment - otherwise the request would be rejected before it reached the vulnerable code. As such, the most likely attacker is an inside user or an attacker that has breached the account of an existing user in the cluster. The issue has been patched in v3.3.1. There is no other mitigation besides upgrading.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46738		
Insertion of Sensitive Information into Log File	03-Jan-2024	6.5	CubeFS is an open-source cloud-native file storage system. CubeFS prior to version 3.3.1 was found to leak users secret keys and access keys in the logs in multiple components. When CubeCS creates new users, it leaks the users secret key. This could allow a lower-privileged user with access to the logs to retrieve sensitive information and impersonate other users with higher privileges than themselves. The issue has been patched in v3.3.1. There is no other mitigation than upgrading CubeFS. **CVE ID : CVE-2023-46742**	https://github.com/cubefs/cubefs/commit/8dcce6ac8dff3db44d7e9074094c7303a5ff5dd	A-LIN-CUBE-290124/360
Observable Discrepancy	03-Jan-2024	5.9	CubeFS is an open-source cloud-native file storage system. A vulnerability was found during in the CubeFS master component in versions prior to	https://github.com/cubefs/cubefs/commit/6a0d5fa45a77ff20c752fa9e44738bf5d86c84bd	A-LIN-CUBE-290124/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.3.1 that could allow an untrusted attacker to steal user passwords by carrying out a timing attack. The root case of the vulnerability was that CubeFS used raw string comparison of passwords. The vulnerable part of CubeFS was the UserService of the master component. The UserService gets instantiated when starting the server of the master component. The issue has been patched in v3.3.1. For impacted users, there is no other way to mitigate the issue besides upgrading. **CVE ID : CVE-2023-46739**		
Vendor: ljapps					
Product: wp_tripadvisor_review_slider					
Affected Version(s): * Up to (excluding) 11.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2024	4.8	The WP TripAdvisor Review Slider WordPress plugin before 11.9 does not sanitise and escape some of its settings, which could allow high	N/A	A-LJA-WP_T-290124/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-6037**		
Vendor: lopalopa					
Product: dynamic_lab_management_system					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	7.5	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin_login_process.php. The manipulation of the argument admin_password 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-249873 was assigned to this vulnerability.	N/A	A-LOP-DYNA-290124/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0306		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	7.5	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login_process.php. The manipulation of the argument password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249874 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0307**	N/A	A-LOP-DYNA-290124/364
Vendor: machothemes					
Product: strong_testimonials					
Affected Version(s): * Up to (including) 3.1.10					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WPChill Strong Testimonials.This issue affects Strong Testimonials: from n/a through 3.1.10.	N/A	A-MAC-STRO-290124/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52123		
Vendor: mappresspro					
Product: mappress					
Affected Version(s): * Up to (excluding) 2.88.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	5.4	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the map title parameter in all versions up to and including 2.88.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6524**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3001436%40mappress-google-maps-for-wordpress%2Ftags%2F2.88.13&new=3015598%40mappress-google-maps-for-wordpress%2Ftags%2F2.88.14#file31	A-MAP-MAPP-290124/366
Vendor: mapster					
Product: mapster_wp_maps					
Affected Version(s): * Up to (including) 1.2.38					
Improper Neutralization of Input	08-Jan-2024	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-MAP-MAPS-290124/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			('Cross-site Scripting') vulnerability in Mapster Technology Inc. Mapster WP Maps allows Stored XSS.This issue affects Mapster WP Maps: from n/a through 1.2.38. **CVE ID : CVE-2024-21744**		
Vendor: mariosalexandrou					
Product: republish_old_posts					
Affected Version(s): * Up to (including) 1.21					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Marios Alexandrou Republish Old Posts.This issue affects Republish Old Posts: from n/a through 1.21. **CVE ID : CVE-2023-52145**	N/A	A-MAR-REPU-290124/368
Vendor: mattermost					
Product: mattermost_server					
Affected Version(s): * Up to (excluding) 8.1.7					
N/A	02-Jan-2024	4.3	Mattermost fails to properly verify the permissions needed for viewing archived public	https://mattermost.com/security-updates	A-MAT-MATT-290124/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			channels, allowing a member of one team to get details about the archived public channels of another team via the GET /api/v4/teams/<team-id>/channels/deleted endpoint. **CVE ID : CVE-2023-47858**		
N/A	02-Jan-2024	4.3	Mattermost fails to scope the WebSocket response around notified users to a each user separately resulting in the WebSocket broadcasting the information about who was notified about a post to everyone else in the channel. **CVE ID : CVE-2023-48732**	https://mattermost.com/security-updates	A-MAT-MATT-290124/370
N/A	02-Jan-2024	4.3	Mattermost fails to update the permissions of the current session for a user who was just demoted to guest, allowing freshly	https://mattermost.com/security-updates	A-MAT-MATT-290124/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			demoted guests to change group names. **CVE ID : CVE-2023-50333**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.5					
N/A	02-Jan-2024	4.3	Mattermost fails to properly verify the permissions needed for viewing archived public channels, allowing a member of one team to get details about the archived public channels of another team via the GET /api/v4/teams/<team-id>/channels/deleted endpoint. **CVE ID : CVE-2023-47858**	https://mattermost.com/security-updates	A-MAT-MATT-290124/372
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.4					
N/A	02-Jan-2024	4.3	Mattermost fails to properly verify the permissions needed for viewing archived public channels, allowing a member of one team to get details about the archived public channels of another team via the GET /api/v4/teams/<team-id>/channels/deleted endpoint.	https://mattermost.com/security-updates	A-MAT-MATT-290124/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47858		
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.3					
N/A	02-Jan-2024	4.3	Mattermost fails to properly verify the permissions needed for viewing archived public channels, allowing a member of one team to get details about the archived public channels of another team via the GET /api/v4/teams/<team-id>/channels/deleted endpoint. **CVE ID : CVE-2023-47858**	https://mattermost.com/security-updates	A-MAT-MATT-290124/374
Vendor: Maxfoundry					
Product: maxbuttons					
Affected Version(s): * Up to (including) 9.7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	4.8	The WordPress Button Plugin MaxButtons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 9.7.4 due to insufficient input sanitization and output escaping. This makes it possible	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3012872%40maxbuttons%2Ftrunk&old=2978023%40maxbuttons%2Ftrunk&sfp_email=&sfph_mail=	A-MAX-MAXB-290124/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. Administrators can give button creation privileges to users with lower levels (contributor+) which would allow those lower-privileged users to carry out attacks. **CVE ID : CVE-2023-6594**		
Vendor: mehah					
Product: otclient					
Affected Version(s): * Up to (excluding) 2023-12-30					
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	02-Jan-2024	9.8	OTCLient is an alternative tibia client for otserv. Prior to commit db560de0b56476c87a2f967466407939196dd254, the /mehah/otclient "`Analysis - SonarCloud`"	https://github.com/mehah/otclient/commit/db560de0b56476c87a2f967466407939196dd254, https://github.com/mehah/otclient/security/advisories/GHSA	A-MEH-OTCL-290124/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			workflow is vulnerable to an expression injection in Actions, allowing an attacker to run commands remotely on the runner, leak secrets, and alter the repository using this workflow. Commit db560de0b56476c87a2f967466407939196dd254 contains a fix for this issue. **CVE ID : CVE-2024-21623**	-q6gr-wc79-v589	
Vendor: meowapps					
Product: database_cleaner					
Affected Version(s): * Up to (including) 0.9.8					
Insertion of Sensitive Information into Log File	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Database Cleaner: Clean, Optimize & Repair.This issue affects Database Cleaner: Clean, Optimize & Repair: from n/a through 0.9.8. **CVE ID : CVE-2023-51508**	N/A	A-MEO-DATA-290124/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: metagauss					
Product: profilegrid					
Affected Version(s): * Up to (including) 5.0.3					
Missing Authorization	08-Jan-2024	8.8	Missing Authorization vulnerability in Profilegrid ProfileGrid – User Profiles, Memberships, Groups and Communities.This issue affects ProfileGrid – User Profiles, Memberships, Groups and Communities: from n/a through 5.0.3. **CVE ID : CVE-2022-36352**	N/A	A-MET-PROF-290124/378
Vendor: michielvaneerd					
Product: private_google_calendars					
Affected Version(s): * Up to (including) 20231125					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michiel van Eerd Private Google Calendars allows Stored XSS.This issue affects Private Google Calendars: from	N/A	A-MIC-PRIV-290124/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 20231125. **CVE ID : CVE-2023-52198**		
Vendor: Microchip					
Product: maxview_storage_manager					
Affected Version(s): From (including) 3.00.23484 Up to (including) 4.14.00.26064					
N/A	08-Jan-2024	9.1	In default installations of Microchip maxView Storage Manager (for Adaptec Smart Storage Controllers) where Redfish server is configured for remote system management, unauthorized access can occur, with data modification and information disclosure. This affects 3.00.23484 through 4.14.00.26064 (except for the patched versions 3.07.23980 and 4.07.00.25339). **CVE ID : CVE-2024-22216**	https://www.microchip.com/en-us/solutions/embedded-security/how-to-report-potential-product-security-vulnerabilities/maxview-storage-manager-redfish-server-vulnerability	A-MIC-MAXV-290124/380
Vendor: Microsoft					
Product: .net					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.26					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	7.5	.NET Denial of Service Vulnerability **CVE ID : CVE-2024-20672**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20672	A-MIC-.NET-290124/381
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.15					
N/A	09-Jan-2024	7.5	.NET Denial of Service Vulnerability **CVE ID : CVE-2024-20672**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20672	A-MIC-.NET-290124/382
Product: .net_framework					
Affected Version(s): 3.5					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/383
Affected Version(s): 4.6.2					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/384
Affected Version(s): 4.7					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/385
Affected Version(s): 4.7.1					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	A-MIC-.NET-290124/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21312	lity/CVE-2024-21312	
Affected Version(s): 4.7.2					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/387
Affected Version(s): 4.8					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/388
Affected Version(s): 4.8.1					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	A-MIC-.NET-290124/389
Product: azure_storage_mover					
Affected Version(s): * Up to (excluding) 3.0.430					
N/A	09-Jan-2024	8	Azure Storage Mover Remote Code Execution Vulnerability **CVE ID : CVE-2024-20676**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20676	A-MIC-AZUR-290124/390
Product: azure_uamqp					
Affected Version(s): * Up to (excluding) 2024-01-01					
Integer Overflow or Wraparound	09-Jan-2024	9.8	Azure uAMQP is a general purpose C library for AMQP 1.0. The UAMQP library is used by several clients to	https://github.com/Azure/azure-uamqp-c/commit/12ddb3a31a5a97f55b06fa5d74c59a	A-MIC-AZUR-290124/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implement AMQP protocol communication. When clients using this library receive a crafted binary type data, an integer overflow or wraparound or memory safety issue can occur and may cause remote code execution. This vulnerability has been patched in release 2024-01-01. **CVE ID : CVE-2024-21646**	1d84ad78fe, https://github.com/Azure/azure-uamqp-c/security/advisories/GHSA-j29m-p99g-7hpv	
Product: printer_metadata_troubleshooter_tool					
Affected Version(s): * Up to (excluding) 1.0.0.1					
N/A	09-Jan-2024	7.8	Microsoft Printer Metadata Troubleshooter Tool Remote Code Execution Vulnerability **CVE ID : CVE-2024-21325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21325	A-MIC-PRIN-290124/392
Product: sharepoint_server					
Affected Version(s): -					
N/A	09-Jan-2024	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2024-21318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318	A-MIC-SHAR-290124/393
Affected Version(s): 2016					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2024-21318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318	A-MIC-SHAR-290124/394
Affected Version(s): 2019					
N/A	09-Jan-2024	8.8	Microsoft SharePoint Server Remote Code Execution Vulnerability **CVE ID : CVE-2024-21318**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318	A-MIC-SHAR-290124/395
Vendor: mojofywp					
Product: wp_affiliate_disclosure					
Affected Version(s): * Up to (including) 1.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MojofyWP WP Affiliate Disclosure allows Stored XSS.This issue affects WP Affiliate Disclosure: from n/a through 1.2.7. **CVE ID : CVE-2023-52178**	N/A	A-MOJ-WP_A-290124/396
Vendor: motopress					
Product: getwid_-_gutenberg_blocks					
Affected Version(s): * Up to (excluding) 2.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jan-2024	7.5	Any unauthenticated user may send e-mail from the site with any title or content to the admin **CVE ID : CVE-2023-6042**	N/A	A-MOT-GETW-290124/397
Vendor: mtrv					
Product: teachpress					
Affected Version(s): * Up to (including) 9.0.4					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.4. **CVE ID : CVE-2023-52129**	N/A	A-MTR-TEAC-290124/398
Vendor: naziinfotech					
Product: ni_purchase_order\(po\)_for_woocommerce					
Affected Version(s): * Up to (including) 1.2.1					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	7.2	The Ni Purchase Order(PO) For WooCommerce WordPress plugin through 1.2.1 does not validate logo and signature image files uploaded in the settings, allowing high privileged user to upload arbitrary files to	N/A	A-NAZ-NI_P-290124/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the web server, triggering an RCE vulnerability by uploading a web shell. **CVE ID : CVE-2023-5957**		
Vendor: ncast_project					
Product: ncast					
Affected Version(s): From (including) 2007 Up to (including) 2017					
N/A	08-Jan-2024	7.5	A vulnerability was found in Guangzhou Yingke Electronic Technology Ncast up to 2017 and classified as problematic. Affected by this issue is some unknown functionality of the file /manage/IPSetup.php of the component Guest Login. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249872. **CVE ID : CVE-2024-0305**	N/A	A-NCA-NCAS-290124/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Netscout					
Product: ngeniusone					
Affected Version(s): 6.3.4					
Improper Restriction of XML External Entity Reference	09-Jan-2024	9.8	An issue found in NetScout nGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted file. **CVE ID : CVE-2023-26999**	N/A	A-NET-NGEN-290124/401
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	6.1	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the name parameter of the Profile and Exclusion List page(s). **CVE ID : CVE-2023-27000**	http://netscout.com/	A-NET-NGEN-290124/402
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the creator parameter of the Alert Configuration page. **CVE ID : CVE-2023-26998**	http://netscout.com/	A-NET-NGEN-290124/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: nia					
Product: rrj_nueva_ecija_engineer_online_portal					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	02-Jan-2024	8.8	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file dasboard_teacher.php of the component Avatar Handler. The manipulation leads to unrestricted upload. 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-249443. **CVE ID : CVE-2024-0185**	N/A	A-NIA-RRJ_-290124/404
Weak Password Requirements	02-Jan-2024	8.1	A vulnerability, which was classified as problematic, was found in RRJ Nueva Ecija Engineer Online Portal 1.0. This affects an unknown part of the file	N/A	A-NIA-RRJ_-290124/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change_password_teacher.php. The manipulation leads to weak password requirements. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-249501 was assigned to this vulnerability. **CVE ID : CVE-2024-0188**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	5.4	A vulnerability has been found in RRJ Nueva Ecija Engineer Online Portal 1.0 and classified as problematic. This vulnerability affects unknown code of the file teacher_message.php of the component Create Message Handler. The manipulation of the argument Content with the input </title><scRipt>alert(x)</scRipt>	N/A	A-NIA-RRJ_-290124/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249502 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0189**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	5.4	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file add_quiz.php of the component Quiz Handler. The manipulation of the argument Quiz Title/Quiz Description with the input </title><scRipt>alert(x)</scRipt> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-NIA-RRJ_-290124/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-249503. **CVE ID : CVE-2024-0190**		
Unrestricted Upload of File with Dangerous Type	02-Jan-2024	5.4	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file downloadable.php of the component Add Downloadable. 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-249505 was assigned to this vulnerability. **CVE ID : CVE-2024-0192**	N/A	A-NIA-RRJ_-290124/408
Insertion of Sensitive Information into Externally-Accessible File or Directory	02-Jan-2024	5.3	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/uploads/.	N/A	A-NIA-RRJ_-290124/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation leads to file and directory information exposure. 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-249504. **CVE ID : CVE-2024-0191**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2024	4.8	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin_user.php of the component Admin Panel. The manipulation of the argument Firstname/Lastname/Username leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-NIA-RRJ_-290124/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB-249433 was assigned to this vulnerability. **CVE ID : CVE-2024-0181**		
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	01-Jan-2024	4.8	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/students.php of the component NIA Office. The manipulation leads to basic 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-249441 was assigned to this vulnerability. **CVE ID : CVE-2024-0183**	N/A	A-NIA-RRJ_-290124/411
Improper Neutralization of Input During Web Page Generation	02-Jan-2024	4.8	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file	N/A	A-NIA-RRJ_-290124/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			/admin/edit_teacher.php of the component Add Enginer. The manipulation of the argument Firstname/Lastname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249442 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0184**		
Vendor: ninjateam					
Product: fastdup					
Affected Version(s): * Up to (including) 2.1.7					
N/A	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FastDup – Fastest WordPress Migration & Duplicator.This issue affects FastDup – Fastest WordPress Migration & Duplicator: from n/a through 2.1.7. **CVE ID : CVE-2023-51406**	N/A	A-NIN-FAST-290124/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: nitropack					
Product: nitropack					
Affected Version(s): * Up to (including) 1.10.2					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in NitroPack Inc. NitroPack – Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images.This issue affects NitroPack – Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images: from n/a through 1.10.2. **CVE ID : CVE-2023-52121**	N/A	A-NIT-NITR-290124/414
Vendor: noorsplugin					
Product: wp_stripe_checkout					
Affected Version(s): * Up to (including) 1.2.2.37					
Insertion of Sensitive Information into Log File	05-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Naa986 WP Stripe Checkout.This issue affects WP Stripe Checkout: from n/a through 1.2.2.37.	N/A	A-NOO-WP_S-290124/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52143		
Vendor: o-ran-sc					
Product: ric-plt-e2mgr					
Affected Version(s): *					
Missing Authorization	03-Jan-2024	7.7	An issue was discovered in O-RAN Software Community ric-plt-e2mgr in the G-Release environment, allows remote attackers to cause a denial of service (DoS) via a crafted request to the E2Manager API component. **CVE ID : CVE-2023-42358**	https://jira.o-ran-sc.org/browse/RIC-1009	A-O-R-RIC--290124/416
Vendor: Ocsinventory-ng					
Product: ocsinventory-ocsreports					
Affected Version(s): 2.12.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.9	OCSInventory allow stored email template with special characters that lead to a Stored cross-site Scripting. **CVE ID : CVE-2023-3726**	N/A	A-OCS-OCSI-290124/417
Vendor: onenav					
Product: onenav					
Affected Version(s): * Up to (including) 0.9.33					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Jan-2024	9.8	A vulnerability was found in OneNav up to 0.9.33. It has been classified as critical. This affects an unknown part of the file /index.php?c=api of the component API. The manipulation of the argument X-Token leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249765 was assigned to this vulnerability. **CVE ID : CVE-2023-7210**	N/A	A-ONE-ONEN-290124/418
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jan-2024	9.8	A vulnerability classified as critical was found in CodeAstro Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /admin/ of the component Admin Panel. The manipulation of the	N/A	A-ONL-ONLI-290124/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249778 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0247**		
Vendor: Open-xchange					
Product: ox_app_suite					
Affected Version(s): * Up to (excluding) 7.10.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jan-2024	9.6	The optional "LDAP contacts provider" could be abused by privileged users to inject LDAP filter strings that allow to access content outside of the intended hierarchy. Unauthorized users could break confidentiality of information in the directory and potentially cause high load on the directory server, leading to denial of service. Encoding has been added for user-provided fragments that are used when	N/A	A-OPE-OX_A-290124/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			constructing the LDAP query. No publicly available exploits are known. **CVE ID : CVE-2023-29050**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	8.8	A component for parsing OXMF templates could be abused to execute arbitrary system commands that would be executed as the non-privileged runtime user. Users and attackers could run system commands with limited privilege to gain unauthorized access to confidential information and potentially violate integrity by modifying resources. The template engine has been reconfigured to deny execution of harmful commands on a system level. No publicly available exploits are known. **CVE ID : CVE-2023-29048**	N/A	A-OPE-OX_A-290124/421
N/A	08-Jan-2024	8.1	User-defined OXMF templates could be used to access a limited part of the	N/A	A-OPE-OX_A-290124/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal OX App Suite Java API. The existing switch to disable the feature by default was not effective in this case. Unauthorized users could discover and modify application state, including objects related to other users and contexts. We now make sure that the switch to disable user-generated templates by default works as intended and will remove the feature in future generations of the product. No publicly available exploits are known. **CVE ID : CVE-2023-29051**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	The "upsell" widget at the portal page could be abused to inject arbitrary script code. Attackers that manage to lure users to a compromised account, or gain temporary access to a legitimate account, could inject script code to gain persistent	N/A	A-OPE-OX_A-290124/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution capabilities under a trusted domain. User input for this widget is now sanitized to avoid malicious content the be processed. No publicly available exploits are known. **CVE ID : CVE-2023-29049**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	User-defined script code could be stored for a upsell related shop URL. This code was not correctly sanitized when adding it to DOM. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known. **CVE ID : CVE-2023-41710**	N/A	A-OPE-OX_A-290124/424
Affected Version(s): 7.10.6					
Improper Neutralization of Special Elements in Output	08-Jan-2024	9.6	The optional "LDAP contacts provider" could be abused by privileged users to inject LDAP filter	N/A	A-OPE-OX_A-290124/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			strings that allow to access content outside of the intended hierarchy. Unauthorized users could break confidentiality of information in the directory and potentially cause high load on the directory server, leading to denial of service. Encoding has been added for user-provided fragments that are used when constructing the LDAP query. No publicly available exploits are known. **CVE ID : CVE-2023-29050**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	8.8	A component for parsing OXMF templates could be abused to execute arbitrary system commands that would be executed as the non-privileged runtime user. Users and attackers could run system commands with limited privilege to gain unauthorized access to confidential information and potentially violate	N/A	A-OPE-OX_A-290124/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity by modifying resources. The template engine has been reconfigured to deny execution of harmful commands on a system level. No publicly available exploits are known. **CVE ID : CVE-2023-29048**		
N/A	08-Jan-2024	8.1	User-defined OXMF templates could be used to access a limited part of the internal OX App Suite Java API. The existing switch to disable the feature by default was not effective in this case. Unauthorized users could discover and modify application state, including objects related to other users and contexts. We now make sure that the switch to disable user-generated templates by default works as intended and will remove the feature in future generations of the product. No	N/A	A-OPE-OX_A-290124/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			publicly available exploits are known. **CVE ID : CVE-2023-29051**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	The "upsell" widget at the portal page could be abused to inject arbitrary script code. Attackers that manage to lure users to a compromised account, or gain temporary access to a legitimate account, could inject script code to gain persistent code execution capabilities under a trusted domain. User input for this widget is now sanitized to avoid malicious content the be processed. No publicly available exploits are known. **CVE ID : CVE-2023-29049**	N/A	A-OPE-OX_A-290124/428
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	Users were able to define disclaimer texts for an upsell shop dialog that would contain script code that was not sanitized correctly. Attackers could lure victims to user accounts with malicious	N/A	A-OPE-OX_A-290124/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known. **CVE ID : CVE-2023-29052**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	5.4	User-defined script code could be stored for a upsell related shop URL. This code was not correctly sanitized when adding it to DOM. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known. **CVE ID : CVE-2023-41710**	N/A	A-OPE-OX_A-290124/430
Affected Version(s): 8.16					
Improper Neutralization of Special Elements in Output Used by a Downstrea	08-Jan-2024	9.6	The optional "LDAP contacts provider" could be abused by privileged users to inject LDAP filter strings that allow to access content	N/A	A-OPE-OX_A-290124/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			outside of the intended hierarchy. Unauthorized users could break confidentiality of information in the directory and potentially cause high load on the directory server, leading to denial of service. Encoding has been added for user-provided fragments that are used when constructing the LDAP query. No publicly available exploits are known. **CVE ID : CVE-2023-29050**		
Affected Version(s): 8.17					
N/A	08-Jan-2024	8.1	User-defined OXMF templates could be used to access a limited part of the internal OX App Suite Java API. The existing switch to disable the feature by default was not effective in this case. Unauthorized users could discover and modify application state, including objects related to other users and	N/A	A-OPE-OX_A-290124/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contexts. We now make sure that the switch to disable user-generated templates by default works as intended and will remove the feature in future generations of the product. No publicly available exploits are known. **CVE ID : CVE-2023-29051**		
Vendor: open5gs					
Product: open5gs					
Affected Version(s): 2.6.6					
Uncontrolled Resource Consumption	02-Jan-2024	7.5	An issue was discovered in open5gs v2.6.6. SIGPIPE can be used to crash AMF. **CVE ID : CVE-2023-50020**	https://github.com/open5gs/open5gs/commit/1aba814938e3a1b2eec7014bf6ce132d34622e08, https://github.com/open5gs/open5gs/issues/2734	A-OPE-OPEN-290124/433
Improper Handling of Exceptional Conditions	02-Jan-2024	5.9	An issue was discovered in open5gs v2.6.6. InitialUEMessage, Registration request sent at a specific time can crash AMF due to incorrect error handling of	https://github.com/open5gs/open5gs/commit/7278714133422cee46c32c7523f81ec2cecad9e2, https://github.com/open5gs/o	A-OPE-OPEN-290124/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nudm_UECM_Registration response. **CVE ID : CVE-2023-50019**	pen5gs/issues/2733	
Vendor: openharmony					
Product: openharmony					
Affected Version(s): * Up to (including) 3.2.2					
Missing Release of Resource after Effective Lifetime	02-Jan-2024	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause DOS through occupy all resources **CVE ID : CVE-2023-47216**	N/A	A-OPE-OPEN-290124/435
Use After Free	02-Jan-2024	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia camera crash through modify a released pointer. **CVE ID : CVE-2023-47857**	N/A	A-OPE-OPEN-290124/436
Use After Free	02-Jan-2024	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia player crash through modify a released pointer.	N/A	A-OPE-OPEN-290124/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48360		
Use After Free	02-Jan-2024	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia player crash through modify a released pointer. **CVE ID : CVE-2023-49135**	N/A	A-OPE-OPEN-290124/438
Use After Free	02-Jan-2024	3.3	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause multimedia audio crash through modify a released pointer. **CVE ID : CVE-2023-49142**	N/A	A-OPE-OPEN-290124/439
Vendor: openkruise					
Product: kruise					
Affected Version(s): From (including) 0.8.0 Up to (excluding) 1.3.1					
Improper Privilege Management	03-Jan-2024	6.5	Kruise provides automated management of large-scale applications on Kubernetes. Starting in version 0.8.0 and prior to versions 1.3.1, 1.4.1, and 1.5.2, an attacker who has gained root privilege of the node that kruise-	https://github.com/openkruise/kruise/security/advisories/GHSA-437m-7hj5-9mpw	A-OPE-KRUI-290124/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			daemon run can leverage the kruise-daemon pod to list all secrets in the entire cluster. After that, the attacker can leverage the "captured" secrets (e.g. the kruise-manager service account token) to gain extra privileges such as pod modification. Versions 1.3.1, 1.4.1, and 1.5.2 fix this issue. A workaround is available. For users that do not require imagepulljob functions, they can modify kruise-daemon-role to drop the cluster level secret get/list privilege. **CVE ID : CVE-2023-30617**		
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.4.1					
Improper Privilege Management	03-Jan-2024	6.5	Kruise provides automated management of large-scale applications on Kubernetes. Starting in version 0.8.0 and prior to versions 1.3.1, 1.4.1, and 1.5.2, an attacker who has gained root	https://github.com/openkruise/kruise/security/advisories/GHSA-437m-7hj5-9mpw	A-OPE-KRUI-290124/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege of the node that kruise-daemon run can leverage the kruise-daemon pod to list all secrets in the entire cluster. After that, the attacker can leverage the "captured" secrets (e.g. the kruise-manager service account token) to gain extra privileges such as pod modification. Versions 1.3.1, 1.4.1, and 1.5.2 fix this issue. A workaround is available. For users that do not require imagepulljob functions, they can modify kruise-daemon-role to drop the cluster level secret get/list privilege. **CVE ID : CVE-2023-30617**		
Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.5.2					
Improper Privilege Management	03-Jan-2024	6.5	Kruise provides automated management of large-scale applications on Kubernetes. Starting in version 0.8.0 and prior to versions 1.3.1, 1.4.1, and 1.5.2, an	https://github.com/openkruise/kruise/security/advisories/GHSA-437m-7hj5-9mpw	A-OPE-KRUI-290124/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who has gained root privilege of the node that kruise-daemon run can leverage the kruise-daemon pod to list all secrets in the entire cluster. After that, the attacker can leverage the "captured" secrets (e.g. the kruise-manager service account token) to gain extra privileges such as pod modification. Versions 1.3.1, 1.4.1, and 1.5.2 fix this issue. A workaround is available. For users that do not require imagepulljob functions, they can modify kruise-daemon-role to drop the cluster level secret get/list privilege. **CVE ID : CVE-2023-30617**		
Vendor: Openvpn					
Product: connect					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.4.6					
Improper Control of Generation of Code	08-Jan-2024	7.8	OpenVPN Connect version 3.0 through 3.4.6 on macOS allows local users to execute code in	N/A	A-OPE-CONN-290124/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			external third party libraries using the DYLD_INSERT_LIBRARIES environment variable **CVE ID : CVE-2023-7224**		
Vendor: oretnom23					
Product: clinic_queuing_system					
Affected Version(s): 1.0					
Authorization Bypass Through User-Controlled Key	07-Jan-2024	9.8	A vulnerability was found in SourceCodester Clinic Queuing System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /LoginRegistration.php. The manipulation of the argument formToken leads to authorization bypass. 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-249820. **CVE ID : CVE-2024-0264**	N/A	A-ORE-CLIN-290124/444
External Control of	07-Jan-2024	8.8	A vulnerability was found in SourceCodester	N/A	A-ORE-CLIN-290124/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File Name or Path			Clinic Queuing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php of the component GET Parameter Handler. The manipulation of the argument page leads to file inclusion. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249821 was assigned to this vulnerability. **CVE ID : CVE-2024-0265**		
Vendor: ovation					
Product: dynamic_content_for_elementor					
Affected Version(s): * Up to (excluding) 2.12.5					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ovation S.R.L. Dynamic Content for Elementor.This issue affects Dynamic Content for Elementor: from n/a before 2.12.5.	N/A	A-OVA-DYNA-290124/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52150		
Vendor: packagekit_project					
Product: packagekit					
Affected Version(s): * Up to (excluding) 1.2.7					
Use After Free	03-Jan-2024	3.3	A use-after-free flaw was found in PackageKitd. In some conditions, the order of cleanup mechanics for a transaction could be impacted. As a result, some memory access could occur on memory regions that were previously freed. Once freed, a memory region can be reused for other allocations and any previously stored data in this memory region is considered lost. **CVE ID : CVE-2024-0217**	https://bugzilla.redhat.com/show_bug.cgi?id=2256624	A-PAC-PACK-290124/447
Vendor: paddlepaddle					
Product: paddlepaddle					
Affected Version(s): * Up to (excluding) 2.6.0					
Out-of-bounds Write	03-Jan-2024	9.8	Stack overflow in paddle.searchsorted in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, or even more damage.	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-013.md	A-PAD-PADD-290124/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52304		
Out-of-bounds Write	03-Jan-2024	9.8	Stack overflow in paddle.linalg.lu_unpack in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, or even more damage. **CVE ID : CVE-2023-52307**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-016.md	A-PAD-PADD-290124/449
Out-of-bounds Write	03-Jan-2024	9.8	Heap buffer overflow in paddle.repeat_interleave in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, information disclosure, or more damage is possible. **CVE ID : CVE-2023-52309**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-018.md	A-PAD-PADD-290124/450
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jan-2024	9.8	PaddlePaddle before 2.6.0 has a command injection in get_online_pass_interval. This resulted in the ability to execute arbitrary commands on the operating system. **CVE ID : CVE-2023-52310**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-019.md	A-PAD-PADD-290124/451
Improper Neutralization of Special Elements	03-Jan-2024	9.8	PaddlePaddle before 2.6.0 has a command injection in _wget_download. This resulted in the	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pd	A-PAD-PADD-290124/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			ability to execute arbitrary commands on the operating system. **CVE ID : CVE-2023-52311**	sa-2023-020.md	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Jan-2024	9.8	PaddlePaddle before 2.6.0 has a command injection in convert_shape_compare. This resulted in the ability to execute arbitrary commands on the operating system. **CVE ID : CVE-2023-52314**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-023.md	A-PAD-PADD-290124/453
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.nanmedian in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38674**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-006.md	A-PAD-PADD-290124/454
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.linalg.matrix_rank in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38675**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-007.md	A-PAD-PADD-290124/455
NULL Pointer Dereference	03-Jan-2024	7.5	Nullptr in paddle.dot in PaddlePaddle before 2.6.0. This	https://github.com/PaddlePaddle/Paddle/blob/develop/securi	A-PAD-PADD-290124/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38676**	ty/advisory/pdsa-2023-008.md	
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.linalg.eig in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38677**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-009.md	A-PAD-PADD-290124/457
Out-of-bounds Read	03-Jan-2024	7.5	OOB access in paddle.mode in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38678**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-010.md	A-PAD-PADD-290124/458
NULL Pointer Dereference	03-Jan-2024	7.5	Nullptr in paddle.nextafter in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52302**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-011.md	A-PAD-PADD-290124/459
NULL Pointer Dereference	03-Jan-2024	7.5	Nullptr in paddle.put_along_axis in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-012.md	A-PAD-PADD-290124/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52303		
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.topk in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52305**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-014.md	A-PAD-PADD-290124/461
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.lerp in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52306**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-015.md	A-PAD-PADD-290124/462
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.amin in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52308**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-017.md	A-PAD-PADD-290124/463
Divide By Zero	03-Jan-2024	7.5	FPE in paddle.argmin and paddle.argmax in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52313**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-022.md	A-PAD-PADD-290124/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.6.0					
NULL Pointer Dereference	03-Jan-2024	7.5	Nullptr dereference in paddle.crop in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-52312**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-021.md	A-PAD-PADD-290124/465
Vendor: pagelayer					
Product: pagelayer					
Affected Version(s): * Up to (including) 1.7.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	5.4	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pagelayer_header_code', 'pagelayer_body_open_code', and 'pagelayer_footer_code' meta fields in all versions up to, and including, 1.7.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above	https://plugins.trac.wordpress.org/browser/pagelayer/trunk/main/post_metas.php#L527, https://plugins.trac.wordpress.org/changeset?old_path=/pagelayer/tags/1.7.8&old=3016486&new_path=/pagelayer/tags/1.7.9&new=3016486&sfp_email=&sfph_mail=	A-PAG-PAGE-290124/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This appears to be a reintroduction of a vulnerability patched in version 1.7.7. **CVE ID : CVE-2023-6738**		
Vendor: payhere					
Product: payhere_payment_gateway					
Affected Version(s): * Up to (excluding) 2.2.12					
Insertion of Sensitive Information into Log File	01-Jan-2024	7.5	The PayHere Payment Gateway WordPress plugin before 2.2.12 automatically creates publicly-accessible log files containing sensitive information when transactions occur. **CVE ID : CVE-2023-6064**	N/A	A-PAY-PAYH-290124/467
Vendor: Pbootcms					
Product: Pbootcms					
Affected Version(s): 3.1.2					
N/A	04-Jan-2024	7.5	Aoyun Technology pbootcms V3.1.2 is vulnerable to Incorrect Access Control, allows remote attackers to gain sensitive information via	N/A	A-PBO-PBOO-290124/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session leakage allows a user to avoid logging into the backend management platform. **CVE ID : CVE-2023-50082**		
Vendor: perfood					
Product: couchauth					
Affected Version(s): * Up to (including) 0.20.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	9.6	A host header injection vulnerability exists in the NPM package @perfood/couch-auth versions <= 0.20.0. By sending a specially crafted host header in the forgot password request, it is possible to send password reset links to users which, once clicked, lead to an attacker-controlled server and thus leak the password reset token. This may allow an attacker to reset other users' passwords and take over their accounts. **CVE ID : CVE-2023-39655**	N/A	A-PER-COUC-290124/469
Vendor: Perl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: Perl					
Affected Version(s): * Up to (excluding) 5.32.1					
Out-of-bounds Write	02-Jan-2024	7.8	A vulnerability was found in Perl. This security issue occurs while Perl for Windows relies on the system path environment variable to find the shell (`cmd.exe`). When running an executable that uses the Windows Perl interpreter, Perl attempts to find and execute `cmd.exe` within the operating system. However, due to path search order issues, Perl initially looks for cmd.exe in the current working directory. This flaw allows an attacker with limited privileges to place`cmd.exe` in locations with weak permissions, such as `C:\ProgramData`. By doing so, arbitrary code can be executed when an administrator attempts to use this executable from these compromised locations.	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1056746	A-PER-PERL-290124/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47039		
Vendor: Phome					
Product: empirecms					
Affected Version(s): 7.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Jan-2024	7.2	SQL injection vulnerability in EmpireCMS v7.5, allows remote attackers to execute arbitrary code and obtain sensitive information via the DoExecSql function. **CVE ID : CVE-2023-50162**	N/A	A-PHO-EMPI-290124/471
Vendor: phpgurukul					
Product: dairy_farm_shop_management_system					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in PHPGurukul Dairy Farm Shop Management System up to 1.1. Affected is an unknown function of the file add-category.php. The manipulation of the argument category leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250122	N/A	A-PHP-DAIR-290124/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0355**		
Product: hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/edit-doctor-specialization.php. The manipulation of the argument doctorspecilization leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250127. **CVE ID : CVE-2024-0360**	N/A	A-PHP-HOSP-290124/473
Improper Neutralization of Special Elements used in an	10-Jan-2024	9.8	A vulnerability classified as critical has been found in PHPGurukul Hospital Management	N/A	A-PHP-HOSP-290124/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			System 1.0. Affected is an unknown function of the file admin/contact.php . The manipulation of the argument mobnum leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250128. **CVE ID : CVE-2024-0361**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability classified as critical was found in PHPGurukul Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/change-password.php. The manipulation of the argument cpass leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-250129 was assigned to this vulnerability. **CVE ID : CVE-2024-0362**	N/A	A-PHP-HOSP-290124/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file admin/patient-search.php. The manipulation of the argument searchdata leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250130 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0363**	N/A	A-PHP-HOSP-290124/476
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file admin/query-details.php. The manipulation of the argument adminremark leads	N/A	A-PHP-HOSP-290124/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250131. **CVE ID : CVE-2024-0364**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	6.1	A vulnerability, which was classified as problematic, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file index.php#contact_us of the component Contact Form. The manipulation of the argument Name/Email/Message leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249843.	N/A	A-PHP-HOSP-290124/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0286		
Vendor: plotly					
Product: plotly.js					
Affected Version(s): * Up to (excluding) 2.25.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	03-Jan-2024	9.8	In Plotly plotly.js before 2.25.2, plot API calls have a risk of __proto__ being polluted in expandObjectPaths or nestedProperty. **CVE ID : CVE-2023-46308**	N/A	A-PLO-PLOT-290124/479
Vendor: presstigers					
Product: simple_job_board					
Affected Version(s): * Up to (including) 2.10.6					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Job Board.This issue affects Simple Job Board: from n/a through 2.10.6. **CVE ID : CVE-2023-52122**	N/A	A-PRE-SIMP-290124/480
Vendor: Prestashop					
Product: prestashop					
Affected Version(s): * Up to (excluding) 1.7.8.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	PrestaShop is an open-source e-commerce platform. Prior to versions 8.1.3 and 1.7.8.11, some event attributes are not detected by the `isCleanHTML`	https://github.com/PrestaShop/PrestaShop/commit/73cfb44666818eefd501b526a894fe884dd12129, https://github.com/PrestaShop	A-PRE-PRES-290124/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method. Some modules using the `isCleanHTML` method could be vulnerable to cross-site scripting. Versions 8.1.3 and 1.7.8.11 contain a patch for this issue. The best workaround is to use the `HTMLPurifier` library to sanitize html input coming from users. The library is already available as a dependency in the PrestaShop project. Beware though that in legacy object models, fields of `HTML` type will call `isCleanHTML`. **CVE ID : CVE-2024-21627**	/PrestaShop/commit/ba06d18466df5b92cb841d504cc7210121104883	
Affected Version(s): * Up to (excluding) 8.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	PrestaShop is an open-source e-commerce platform. Prior to version 8.1.3, the isCleanHtml method is not used on this this form, which makes it possible to store a cross-site scripting payload in the database. The impact is low	https://github.com/PrestaShop/PrestaShop/commit/c3d78b7e49f5fe49a9d07725c3174d005deaa597, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-vr7m-r9vm-m4wf	A-PRE-PRES-290124/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the HTML is not interpreted in BO, thanks to twig's escape mechanism. In FO, the cross-site scripting attack is effective, but only impacts the customer sending it, or the customer session from which it was sent. This issue affects those who have a module fetching these messages from the DB and displaying it without escaping HTML. Version 8.1.3 contains a patch for this issue. **CVE ID : CVE-2024-21628**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	PrestaShop is an open-source e-commerce platform. Prior to versions 8.1.3 and 1.7.8.11, some event attributes are not detected by the `isCleanHTML` method. Some modules using the `isCleanHTML` method could be vulnerable to cross-site scripting. Versions 8.1.3 and 1.7.8.11 contain a patch for this issue.	https://github.com/PrestaShop/PrestaShop/commit/73cfb44666818eefd501b526a894fe884dd12129, https://github.com/PrestaShop/PrestaShop/commit/ba06d18466df5b92cb841d504cc7210121104883	A-PRE-PRES-290124/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The best workaround is to use the `HTMLPurifier` library to sanitize html input coming from users. The library is already available as a dependency in the PrestaShop project. Beware though that in legacy object models, fields of `HTML` type will call `isCleanHTML`. **CVE ID : CVE-2024-21627**		
Vendor: prestashow					
Product: google_integrator					
Affected Version(s): * Up to (excluding) 2.1.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	9.1	Blind SQL Injection vulnerability in PrestaShow Google Integrator (PrestaShop addon) allows for data extraction and modification. This attack is possible via command insertion in one of the cookies. **CVE ID : CVE-2023-6921**	N/A	A-PRE-GOOG-290124/484
Vendor: priva					
Product: top_control_suite					
Affected Version(s): * Up to (including) 8.7.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Password Hash With Insufficient Computational Effort	02-Jan-2024	7.5	The Priva TopControl Suite contains predictable credentials for the SSH service, based on the Serial number. Which makes it possible for an attacker to calculate the login credentials for the Priva TopControll suite. **CVE ID : CVE-2022-3010**	N/A	A-PRI-TOP_-290124/485
Vendor: projectworlds					
Product: online_job_portal					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	4.8	A vulnerability was found in Online Job Portal 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Admin/News.php of the component Create News Page. The manipulation of the argument News with the input </title><scRipt>alert(0x00C57D)</scRipt> leads to cross site scripting. The attack may be launched remotely. The exploit has	N/A	A-PRO-ONLI-290124/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. VDB-249818 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0262**		
Vendor: puma					
Product: puma					
Affected Version(s): * Up to (excluding) 5.6.8					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Jan-2024	7.5	Puma is a web server for Ruby/Rack applications built for parallelism. Prior to version 6.4.2, puma exhibited incorrect behavior when parsing chunked transfer encoding bodies in a way that allowed HTTP request smuggling. Fixed versions limits the size of chunk extensions. Without this limit, an attacker could cause unbounded resource (CPU, network bandwidth) consumption. This vulnerability has been fixed in versions 6.4.2 and 5.6.8. **CVE ID : CVE-2024-21647**	https://github.com/puma/puma/commit/5fc43d73b6ff193325e657a24ed76dec79133e93, https://github.com/puma/puma/security/advisories/GHSA-c2f4-cvqm-65w2	A-PUM-PUMA-290124/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.4.2					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	08-Jan-2024	7.5	Puma is a web server for Ruby/Rack applications built for parallelism. Prior to version 6.4.2, puma exhibited incorrect behavior when parsing chunked transfer encoding bodies in a way that allowed HTTP request smuggling. Fixed versions limits the size of chunk extensions. Without this limit, an attacker could cause unbounded resource (CPU, network bandwidth) consumption. This vulnerability has been fixed in versions 6.4.2 and 5.6.8. **CVE ID : CVE-2024-21647**	https://github.com/puma/puma/commit/5fc43d73b6ff193325e657a24ed76dec79133e93, https://github.com/puma/puma/security/advisories/GHSA-c2f4-cvqm-65w2	A-PUM-PUMA-290124/488
Vendor: pycryptodome					
Product: pycryptodome					
Affected Version(s): * Up to (excluding) 3.19.1					
Observable Discrepancy	05-Jan-2024	5.9	PyCryptodome and pycryptodomex before 3.19.1 allow side-channel leakage for OAEP decryption, exploitable for a Manger attack.	N/A	A-PYC-PYCR-290124/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52323		
Product: pycryptodomex					
Affected Version(s): * Up to (excluding) 3.19.1					
Observable Discrepancy	05-Jan-2024	5.9	PyCryptodome and pycryptodomex before 3.19.1 allow side-channel leakage for OAEP decryption, exploitable for a Manger attack. **CVE ID : CVE-2023-52323**	N/A	A-PYC-PYCR-290124/490
Vendor: pyload					
Product: pyload					
Affected Version(s): 0.5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.8	pyLoad 0.5.0 is vulnerable to Unrestricted File Upload. **CVE ID : CVE-2023-47890**	N/A	A-PYL-PYLO-290124/491
N/A	08-Jan-2024	7.5	pyLoad is the free and open-source Download Manager written in pure Python. Any unauthenticated user can browse to a specific URL to expose the Flask config, including the `SECRET_KEY` variable. This issue has been patched in version 0.5.0b3.dev77.	https://github.com/pyload/pyload/commit/bb22063a875ffeca357aaf6e2edcd09705688c40, https://github.com/pyload/pyload/security/advisories/GHSA-mqpq-2p68-46fv	A-PYL-PYLO-290124/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21644		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jan-2024	5.3	pyLoad is the free and open-source Download Manager written in pure Python. A log injection vulnerability was identified in `pyload` allowing any unauthenticated actor to inject arbitrary messages into the logs gathered by `pyload`. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to implicate another party in the commission of a malicious act. This vulnerability has been patched in version 0.5.0b3.dev77. **CVE ID : CVE-2024-21645**	https://github.com/pyload/pyload/commit/4159a1191ec4fe6d927e57a9c4bb8f54e16c381d, https://github.com/pyload/pyload/security/advisories/GHSA-ghmw-rwh8-6qmr	A-PYL-PYLO-290124/493
Affected Version(s): * Up to (including) 0.4.9					
N/A	08-Jan-2024	7.5	pyLoad is the free and open-source Download Manager written in pure Python. Any unauthenticated user can browse to	https://github.com/pyload/pyload/commit/bb22063a875ffeca357aaf6e2edcd09705688c40, https://github.c	A-PYL-PYLO-290124/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a specific URL to expose the Flask config, including the `SECRET_KEY` variable. This issue has been patched in version 0.5.0b3.dev77. **CVE ID : CVE-2024-21644**	om/pyload/pyload/security/advisories/GHSA-mqpq-2p68-46fv	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Jan-2024	5.3	pyLoad is the free and open-source Download Manager written in pure Python. A log injection vulnerability was identified in `pyload` allowing any unauthenticated actor to inject arbitrary messages into the logs gathered by `pyload`. Forged or otherwise, corrupted log files can be used to cover an attacker's tracks or even to implicate another party in the commission of a malicious act. This vulnerability has been patched in version 0.5.0b3.dev77. **CVE ID : CVE-2024-21645**	https://github.com/pyload/pyload/commit/4159a1191ec4fe6d927e57a9c4bb8f54e16c381d, https://github.com/pyload/pyload/security/advisories/GHSA-ghmw-rwh8-6qmr	A-PYL-PYLO-290124/495
Vendor: Qemu					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qemu					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	5.3	A stack based buffer overflow was found in the virtio-net device of QEMU. This issue occurs when flushing TX in the virtio_net_flush_tx function if guest features VIRTIO_NET_F_HASH_REPORT, VIRTIO_F_VERSION_1 and VIRTIO_NET_F_MRG_RXBUF are enabled. This could allow a malicious user to overwrite local variables allocated on the stack. Specifically, the `out_sg` variable could be used to read a part of process memory and send it to the wire, causing an information leak. **CVE ID : CVE-2023-6693**	https://bugzilla.redhat.com/show_bug.cgi?id=2254580	A-QEM-QEMU-290124/496
Vendor: Qnap					
Product: qcalagent					
Affected Version(s): From (including) 1.1.0 Up to (excluding) 1.1.8					
Improper Neutralization of Special Elements used in an	05-Jan-2024	8.8	An OS command injection vulnerability has been reported to affect QcalAgent. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-34	A-QNA-QCAL-290124/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QcalAgent 1.1.8 and later **CVE ID : CVE-2023-41289**		
Product: qumagie					
Affected Version(s): 2.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Jan-2024	8.8	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later **CVE ID : CVE-2023-47219**	https://www.qnap.com/en/security-advisory/qsa-23-32	A-QNA-QUMA-290124/498
Improper Neutralization of Special Elements used in a	05-Jan-2024	8.8	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-23	A-QNA-QUMA-290124/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later **CVE ID : CVE-2023-47560**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	5.4	A cross-site scripting (XSS) vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later **CVE ID : CVE-2023-47559**	https://www.qnap.com/en/security-advisory/qsa-23-23	A-QNA-QUMA-290124/500
Product: video_station					
Affected Version(s): From (including) 5.7.0 Up to (excluding) 5.7.2					
Improper Neutralization of Special Elements	05-Jan-2024	8.8	A SQL injection vulnerability has been reported to affect Video Station. If	https://www.qnap.com/en/security-	A-QNA-VIDE-290124/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later **CVE ID : CVE-2023-41287**	advisory/qsa-23-55	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	8.8	An OS command injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later **CVE ID : CVE-2023-41288**	https://www.qnap.com/en/security-advisory/qsa-23-55	A-QNA-VIDE-290124/502
Vendor: qualys					
Product: policy_compliance					
Affected Version(s): * Up to (including) 1.0.5					
Improper Restriction of XML	09-Jan-2024	6.5	Qualys Jenkins Plugin for Policy	https://www.qualys.com/security-advisories/	A-QUA-POLI-290124/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data **CVE ID : CVE-2023-6147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	Qualys Jenkins Plugin for Policy Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check	https://www.qualys.com/security-advisories/	A-QUA-POLI-290124/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to Qualys Cloud Services. This allowed any user with login access and access to configure or edit jobs to utilize the plugin to configure a potential rouge endpoint via which it was possible to control response for certain request which could be injected with XSS payloads leading to XSS while processing the response data **CVE ID : CVE-2023-6148**		
Product: web_application_screening					
Affected Version(s): * Up to (including) 2.0.11					
Improper Restriction of XML External Entity Reference	09-Jan-2024	6.5	Qualys Jenkins Plugin for WAS prior to version and including 2.0.11 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit	https://www.qualys.com/security-advisories/	A-QUA-WEB_-290124/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data **CVE ID : CVE-2023-6149**		
Vendor: really-simple-plugins					
Product: complianz					
Affected Version(s): * Up to (including) 6.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	4.8	The Complianz – GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to and including 6.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3009228%40complianz-gdpr&new=3009228%40complianz-gdpr&sfp_email=&sfph_mail=	A-REA-COMP-290124/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-6498**		
Vendor: recognizeapp					
Product: omniauth					
Affected Version(s): \\ Up to (excluding) 2.0.0					
Improper Authentication	02-Jan-2024	9.8	omniauth-microsoft_graph provides an Omniauth strategy for the Microsoft Graph API. Prior to versions 2.0.0, the implementation did not validate the legitimacy of the `email` attribute of the user nor did it give/document an option to do so, making it susceptible to nOAuth misconfiguration in cases when the `email` is used as a trusted user identifier. This could lead to account takeover. Version 2.0.0 contains a fix for this issue.	https://github.com/synth/omniauth-microsoft_graph/commit/f132078389612b797c872b45bd0e0b47382414c1, https://github.com/synth/omniauth-microsoft_graph/security/advisories/GHSA-5g66-628f-7cvj	A-REC-OMNI-290124/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21632		
Vendor: Redhat					
Product: red_hat_developer_hub					
Affected Version(s): * Up to (excluding) 1.21.0					
Generation of Error Message Containing Sensitive Information	04-Jan-2024	5.7	A flaw was found in the Red Hat Developer Hub (RHDH). The catalog-import function leaks GitLab access tokens on the frontend when the base64 encoded GitLab token includes a newline at the end of the string. The sanitized error can display on the frontend, including the raw access token. Upon gaining access to this token and depending on permissions, an attacker could push malicious code to repositories, delete resources in Git, revoke or generate new keys, and sign code illegitimately. **CVE ID : CVE-2023-6944**	https://access.redhat.com/security/cve/CVE-2023-6944, https://bugzilla.redhat.com/show_bug.cgi?id=2255204	A-RED-RED_-290124/508
Vendor: reputeinfosystems					
Product: armember					
Affected Version(s): * Up to (including) 4.0.22					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Jan-2024	9.8	Cross-Site Request Forgery (CSRF), Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup.This issue affects ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup: n/a. **CVE ID : CVE-2023-52200**	N/A	A-REP-ARME-290124/509
Vendor: royaltechbd					
Product: royal_prettyphoto					
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	A vulnerability was found in rt-prettyphoto Plugin up to 1.2 on WordPress and classified as problematic. Affected by this issue is the function royal_prettyphoto_plugin_links of the file rt-prettyphoto.php. The manipulation leads to cross site	https://github.com/wp-plugins/rt-prettyphoto/commit/0d3d38cfa487481b66869e4212df1cefc281ecb7	A-ROY-ROYA-290124/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack may be launched remotely. Upgrading to version 1.3 is able to address this issue. The patch is identified as 0d3d38cfa487481b66869e4212df1cefc281ecb7. It is recommended to upgrade the affected component. VDB-249422 is the identifier assigned to this vulnerability. **CVE ID : CVE-2015-10128**		
Vendor: rust-vmm					
Product: vmm-sys-util					
Affected Version(s): From (including) 0.5.0 Up to (excluding) 0.12.0					
Out-of-bounds Write	02-Jan-2024	9.8	vmm-sys-util is a collection of modules that provides helpers and utilities used by multiple rust-vmm components. Starting in version 0.5.0 and prior to version 0.12.0, an issue in the `FamStructWrapper::deserialize` implementation provided by the crate for `vmm_sys_util::fam::FamStructWrappe	https://github.com/rust-vmm/vmm-sys-util/commit/30172fca2a8e0a38667d934ee56682247e13f167, https://github.com/rust-vmm/vmm-sys-util/security/advisories/GHSA-875g-mfp6-g7f9	A-RUS-VMM--290124/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r` can lead to out of bounds memory accesses. The deserialization does not check that the length stored in the header matches the flexible array length. Mismatch in the lengths might allow out of bounds memory access through Rust-safe methods. The issue was corrected in version 0.12.0 by inserting a check that verifies the lengths of compared flexible arrays are equal for any deserialized header and aborting deserialization otherwise. Moreover, the API was changed so that header length can only be modified through Rust-unsafe code. This ensures that users cannot trigger out-of-bounds memory access from Rust-safe code. **CVE ID : CVE-2023-50711**		
Vendor: rymera					
Product: wholesale_suite					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.1.5					
Missing Authorization	08-Jan-2024	8.8	Missing Authorization vulnerability in Rymera Web Co Wholesale Suite – WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More.This issue affects Wholesale Suite – WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More: from n/a through 2.1.5. **CVE ID : CVE-2022-34344**	N/A	A-RYM-WHOL-290124/512
Vendor: S-cms					
Product: S-cms					
Affected Version(s): 5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	6.5	S-CMS v5.0 was discovered to contain an arbitrary file read vulnerability. **CVE ID : CVE-2023-29962**	N/A	A-S-C-S-CM-290124/513
Vendor: Samsung					
Product: dex					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) smr_jan-2024_release_1					
N/A	04-Jan-2024	5.5	Improper access control vulnerability in Samsung DeX prior to SMR Jan-2024 Release 1 allows owner to access other users' notification in a multi-user environment. **CVE ID : CVE-2024-20802**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	A-SAM-DEX-290124/514
Product: email					
Affected Version(s): * Up to (excluding) 6.1.90.16					
N/A	04-Jan-2024	3.3	Implicit intent hijacking vulnerability in Samsung Email prior to version 6.1.90.16 allows attacker to get sensitive information. **CVE ID : CVE-2024-20807**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=01	A-SAM-EMAI-290124/515
Product: myfiles					
Affected Version(s): * Up to (excluding) 14.5.00.21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	A-SAM-MYFI-290124/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20804		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2024-20805**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	A-SAM-MYFI-290124/517
Product: nearby_device_scanning					
Affected Version(s): * Up to (excluding) 11.1.14.7					
N/A	04-Jan-2024	5.5	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data. **CVE ID : CVE-2024-20808**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=01	A-SAM-NEAR-290124/518
N/A	04-Jan-2024	5.5	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data. **CVE ID : CVE-2024-20809**	https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=01	A-SAM-NEAR-290124/519
Vendor: SAP					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gui_connector					
Affected Version(s): 1.0					
N/A	09-Jan-2024	7.5	Under certain conditions the Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) - version 1.0, allows an attacker to access highly sensitive information which would otherwise be restricted causing high impact on confidentiality. **CVE ID : CVE-2024-22125**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-GUI_-290124/520
Product: lt_replication_server					
Affected Version(s): s4core_103					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LT_R-290124/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has High impact on confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**		
Affected Version(s): s4core_104					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LT_R-290124/522
Affected Version(s): s4core_105					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-LT_R-290124/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**	c68f7e60039b.html	
Affected Version(s): s4core_106					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LT_R-290124/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**		
Affected Version(s): s4core_107					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LT_R-290124/525
Affected Version(s): s4core_108					
Incorrect Authorization	09-Jan-2024	7.2	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LT_R-290124/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system. **CVE ID : CVE-2024-21735**		
Product: marketing					
Affected Version(s): 160					
URL Redirection to Untrusted Site ('Open Redirect')	09-Jan-2024	5.4	SAP Marketing (Contacts App) - version 160, allows an attacker with low privileges to trick a user to open malicious page which could lead to a very convincing phishing attack with low impact on confidentiality and integrity of the application. **CVE ID : CVE-2024-21734**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-MARK-290124/527
Product: netweaver_application_server_abap					
Affected Version(s): 700					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/528
Affected Version(s): 701					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21738		
Affected Version(s): 702					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/530
Affected Version(s): 731					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 740					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/532
Affected Version(s): 750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the application data after successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 751					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/534
Affected Version(s): 752					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 753					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/536
Affected Version(s): 754					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 755					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/538
Affected Version(s): 756					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS)	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 757					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/540
Affected Version(s): 758					
Improper Neutralization of Input During Web Page Generation	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**		
Affected Version(s): 79					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-290124/542
Affected Version(s): 793					
Improper Neutralizat	09-Jan-2024	5.4	SAP NetWeaver ABAP Application	https://www.sap.com/documen	A-SAP-NETW-290124/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation. **CVE ID : CVE-2024-21738**	ts/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Vendor: servit					
Product: affiliate-toolkit					
Affected Version(s): * Up to (excluding) 3.4.3					
Missing Authorization	01-Jan-2024	9.8	The affiliate-toolkit WordPress plugin before 3.4.3 lacks authorization and authentication for requests to it's affiliate-toolkit-starter/tools/atkp_imagereceiver.php endpoint, allowing unauthenticated visitors to make requests to arbitrary URL's, including RFC1918 private addresses, leading to a Server Side Request	N/A	A-SER-AFFI-290124/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Forgery (SSRF) issue. **CVE ID : CVE-2023-5877**		
Vendor: shapedplugin					
Product: wp_tabs					
Affected Version(s): * Up to (including) 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2024	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC WP Tabs – Responsive Tabs Plugin for WordPress allows Stored XSS.This issue affects WP Tabs – Responsive Tabs Plugin for WordPress: from n/a through 2.2.0. **CVE ID : CVE-2023-52124**	N/A	A-SHA-WP_T-290124/545
Vendor: sidequestvr					
Product: sidequest					
Affected Version(s): * Up to (excluding) 0.10.35					
Improper Input Validation	04-Jan-2024	8.8	SideQuest is a place to get virtual reality applications for Oculus Quest. The SideQuest desktop application uses deep links with a	https://github.com/SideQuestVR/SideQuest/security/advisories/GHSA-3v86-cf9q-x4x7	A-SID-SIDE-290124/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			custom protocol (`sidequest://`) to trigger actions in the application from its web contents. Because, prior to version 0.10.35, the deep link URLs were not sanitized properly in all cases, a one-click remote code execution can be achieved in cases when a device is connected, the user is presented with a malicious link and clicks it from within the application. As of version 0.10.35, the custom protocol links within the electron application are now being parsed and sanitized properly. **CVE ID : CVE-2024-21625**		
Vendor: Siemens					
Product: jt2go					
Affected Version(s): * Up to (excluding) 14.3.0.6					
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13),	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-JT2G-290124/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51439**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-JT2G-290124/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51745**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-JT2G-290124/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51746**		
NULL Pointer Dereference	09-Jan-2024	5.5	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-JT2G-290124/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition. **CVE ID : CVE-2023-51744**		
Product: simatic_cn_4100					
Affected Version(s): * Up to (excluding) 2.7					
Authorization Bypass Through User-Controlled Key	09-Jan-2024	9.8	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up. **CVE ID : CVE-2023-49251**	https://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf	A-SIE-SIMA-290124/551
N/A	09-Jan-2024	9.8	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application uses default credential with admin privileges. An	https://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf	A-SIE-SIMA-290124/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could use the credentials to gain complete control of the affected device. **CVE ID : CVE-2023-49621**		
N/A	09-Jan-2024	7.5	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2023-49252**	https://cert-portal.siemens.com/productcert/pdf/ssa-777015.pdf	A-SIE-SIMA-290124/553
Product: solid_edge_se2023					
Affected Version(s): * Up to (excluding) 223.0					
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49121		
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49122**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/555
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49123**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49124**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/557
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49126**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49127**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/559
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49128**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49129**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/561
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49130**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49131**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/563
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49132**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 223.0					
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49121**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/565
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49122**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/566
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023	https://cert-portal.siemens.com/productcert	A-SIE-SOLI-290124/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49123**	/pdf/ssa-589891.pdf	
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49124**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/568
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/569

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 PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49126**		
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). 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-2023-49127**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/570
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-49128**		
Out-of-bounds Write	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-49129**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/572
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49130**		
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49131**	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/574
Access of Uninitialized Pointer	09-Jan-2024	7.8	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted	https://cert-portal.siemens.com/productcert/pdf/ssa-589891.pdf	A-SIE-SOLI-290124/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. **CVE ID : CVE-2023-49132**		
Product: teamcenter_visualization					
Affected Version(s): From (including) 13.3.0 Up to (excluding) 13.3.0.13					
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-51439**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51745**	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/577
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter	https://cert-portal.siemens.com/productcert	A-SIE-TEAM-290124/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51746**	/pdf/ssa-794653.pdf	
NULL Pointer Dereference	09-Jan-2024	5.5	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition. **CVE ID : CVE-2023-51744**		
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.0.12					
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51439**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51745**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51746**	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	09-Jan-2024	5.5	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition. **CVE ID : CVE-2023-51744**	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/583
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.0.9					
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51439**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12),	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51745**		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51746**		
NULL Pointer Dereference	09-Jan-2024	5.5	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to crash the application causing denial of service condition. **CVE ID : CVE-2023-51744**		
Affected Version(s): From (including) 14.3 Up to (excluding) 14.3.0.6					
Out-of-bounds Read	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51439		
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51745**	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/589
Stack-based Buffer Overflow	09-Jan-2024	7.8	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process. **CVE ID : CVE-2023-51746**		
NULL Pointer Dereference	09-Jan-2024	5.5	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9),	https://cert-portal.siemens.com/productcert/pdf/ssa-794653.pdf	A-SIE-TEAM-290124/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition. **CVE ID : CVE-2023-51744**		
Vendor: siemens-healthineers					
Product: syngo_fastview					
Affected Version(s): *					
Out-of-bounds Write	04-Jan-2024	7.8	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing DICOM files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to	https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-688797	A-SIE-SYNG-290124/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. (ZDI-CAN-15097) **CVE ID : CVE-2021-40367**		
Out-of-bounds Write	04-Jan-2024	7.8	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing BMP files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14860) **CVE ID : CVE-2021-42028**	https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-688797	A-SIE-SYNG-290124/593
Write-what-where Condition	04-Jan-2024	7.8	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing BMP files. This could result in a write-what-where condition and an	https://www.siemens-healthineers.com/en-us/support-documentation/cybersecurity/shsa-688797	A-SIE-SYNG-290124/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15696) **CVE ID : CVE-2021-45465**		
Vendor: silabs					
Product: gecko_software_development_kit					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 4.4.0					
Missing Initialization of Resource	03-Jan-2024	6.8	Glitch detection is not enabled by default for the CortexM33 core in Silicon Labs secure vault high parts EFx32xG2xB, except EFR32xG21B. **CVE ID : CVE-2023-5138**	N/A	A-SIL-GECK-290124/595
Affected Version(s): From (including) 1.0.0 Up to (including) 4.3.2					
N/A	02-Jan-2024	9.8	An unvalidated input in Silicon Labs TrustZone implementation in v4.3.x and earlier of the Gecko SDK allows an attacker to access the trusted region of memory from the untrusted region. **CVE ID : CVE-2023-4280**	N/A	A-SIL-GECK-290124/596
Vendor: simple_house_rental_system_project					
Product: simple_house_rental_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	6.1	A vulnerability classified as problematic was found in CodeAstro Simple House Rental System 5.6. Affected by this vulnerability is an unknown functionality of the component Login Panel. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250111. **CVE ID : CVE-2024-0343**	N/A	A-SIM-SIMP-290124/597
Vendor: smashballoon					
Product: custom_twitter_feeds					
Affected Version(s): * Up to (including) 2.1.2					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Custom Twitter Feeds – A Tweets Widget or X Feed Widget.This issue affects Custom Twitter Feeds – A Tweets Widget or X	N/A	A-SMA-CUST-290124/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feed Widget: from n/a through 2.1.2. **CVE ID : CVE-2023-52136**		
Vendor: snapcreek					
Product: duplicator					
Affected Version(s): * Up to (excluding) 1.3.0					
N/A	08-Jan-2024	9.8	The Duplicator WordPress plugin before 1.3.0 does not properly escape values when its installer script replaces values in WordPress configuration files. If this installer script is left on the site after use, it could be use to run arbitrary code on the server. **CVE ID : CVE-2018-25095**	N/A	A-SNA-DUPL-290124/599
Vendor: spassarop					
Product: owasp_antisamy_.net					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	6.1	OWASP AntiSamy .NET is a library for performing cleansing of HTML coming from untrusted sources. Prior to version 1.2.0, there is a potential for a mutation cross-site	https://github.com/spassarop/antisamy-dotnet/commit/7e500daef6ad9c10e97c68feab78f4cb6e3083c6, https://github.com/spassarop/	A-SPA-OWAS-290124/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting (mXSS) vulnerability in AntiSamy caused by flawed parsing of the HTML being sanitized. To be subject to this vulnerability the `preserveComments` directive must be enabled in your policy file and also allow for certain tags at the same time. As a result, certain crafty inputs can result in elements in comment tags being interpreted as executable when using AntiSamy's sanitized output. This is patched in OWASP AntiSamy .NET 1.2.0 and later. See important remediation details in the reference given below. As a workaround, manually edit the AntiSamy policy file (e.g., antisamy.xml) by deleting the `preserveComments` directive or setting its value to `false`, if present. Also it would be useful to make AntiSamy remove	antisamy-dotnet/commit/8117911933e75a25cd0054ef017577486338444a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `noscript` tag by adding a line described in the GitHub Security Advisory to the tag definitions under the `<tagrules>` node, or deleting it entirely if present. As the previously mentioned policy settings are preconditions for the mXSS attack to work, changing them as recommended should be sufficient to protect you against this vulnerability when using a vulnerable version of this library. However, the existing bug would still be present in AntiSamy or its parser dependency (HtmlAgilityPack). The safety of this workaround relies on configurations that may change in the future and don't address the root cause of the vulnerability. As such, it is strongly recommended to upgrade to a fixed version of AntiSamy.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51652		
Vendor: Spip					
Product: spip					
Affected Version(s): * Up to (excluding) 4.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.1	ecrire/public/assembler.php in SPIP before 4.1.3 and 4.2.x before 4.2.7 allows XSS because input from _request() is not restricted to safe characters such as alphanumerics. **CVE ID : CVE-2023-52322**	https://git.spip.net/spip/spip/commit/e90f5344b8c82711053053e778d38a35e42b7bcb	A-SPI-SPIP-290124/601
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.1	ecrire/public/assembler.php in SPIP before 4.1.3 and 4.2.x before 4.2.7 allows XSS because input from _request() is not restricted to safe characters such as alphanumerics. **CVE ID : CVE-2023-52322**	https://git.spip.net/spip/spip/commit/e90f5344b8c82711053053e778d38a35e42b7bcb	A-SPI-SPIP-290124/602
Vendor: sssssss					
Product: magic-api					
Affected Version(s): * Up to (including) 2.0.1					
Improper Control of Generation of Code ('Code Injection')	02-Jan-2024	8.8	A vulnerability has been found in Magic-Api up to 2.0.1 and classified as critical. Affected by this vulnerability is an	N/A	A-SSS-MAGI-290124/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown functionality of the file /resource/file/api/save?auto=1. The manipulation leads to code 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-249511. **CVE ID : CVE-2024-0196**		
Product: spider-flow					
Affected Version(s): 0.4.3					
Improper Control of Generation of Code ('Code Injection')	02-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in spider-flow 0.4.3. Affected is the function FunctionService.saveFunction of the file src/main/java/org/spiderflow/controller/FunctionController.java. The manipulation leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	N/A	A-SSS-SPID-290124/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-249510 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0195**		
Vendor: ST					
Product: x-cube-safea1					
Affected Version(s): 1.2.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Jan-2024	7.5	STMicroelectronics STSAFE-A1xx middleware before 3.3.7 allows MCU code execution if an adversary has the ability to read from and write to the I2C bus. This is caused by an StSafeA_ReceiveBytes buffer overflow in the X-CUBE-SAFEA1 Software Package for STSAFE-A sample applications (1.2.0), and thus can affect user-written code that was derived from a published sample application. **CVE ID : CVE-2023-50096**	N/A	A-ST-X-CU-290124/605
Vendor: studiowombat					
Product: wp_optin_wheel					
Affected Version(s): * Up to (including) 1.4.3					
Insertion of Sensitive Informatio	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized	N/A	A-STU-WP_O-290124/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			Actor vulnerability in StudioWombat WP Optin Wheel – Gamified Optin Email Marketing Tool for WordPress and WooCommerce.This issue affects WP Optin Wheel – Gamified Optin Email Marketing Tool for WordPress and WooCommerce: from n/a through 1.4.3. **CVE ID : CVE-2023-51408**		
Vendor: studip					
Product: stud.ip					
Affected Version(s): * Up to (excluding) 5.0.9					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	9	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the www-data user. The fixed versions	N/A	A-STU-STUD-290124/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 5.3.4, 5.2.6, 5.1.7, and 5.0.9. **CVE ID : CVE-2023-50982**		
Affected Version(s): From (including) 5.1 Up to (excluding) 5.1.7					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	9	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the www-data user. The fixed versions are 5.3.4, 5.2.6, 5.1.7, and 5.0.9. **CVE ID : CVE-2023-50982**	N/A	A-STU-STUD-290124/608
Affected Version(s): From (including) 5.2 Up to (excluding) 5.2.6					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	9	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the	N/A	A-STU-STUD-290124/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			www-data user. The fixed versions are 5.3.4, 5.2.6, 5.1.7, and 5.0.9. **CVE ID : CVE-2023-50982**		
Affected Version(s): From (including) 5.3 Up to (excluding) 5.3.4					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	9	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the www-data user. The fixed versions are 5.3.4, 5.2.6, 5.1.7, and 5.0.9. **CVE ID : CVE-2023-50982**	N/A	A-STU-STUD-290124/610
Vendor: stylishpricelist					
Product: stylish_price_list					
Affected Version(s): * Up to (including) 7.0.17					
N/A	05-Jan-2024	9.8	Cross-Site Request Forgery (CSRF) vulnerability in Designful Stylish Price List – Price Table Builder & QR Code Restaurant Menu.This issue affects Stylish Price List – Price Table	N/A	A-STY-STYL-290124/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Builder & QR Code Restaurant Menu: from n/a through 7.0.17. **CVE ID : CVE-2023-51673**		
Vendor: Subnet					
Product: powersystem_center					
Affected Version(s): 2020					
Unquoted Search Path or Element	08-Jan-2024	7.8	PowerSYSTEM Center versions 2020 Update 16 and prior contain a vulnerability that may allow an authorized local user to insert arbitrary code into the unquoted service path and escalate privileges. **CVE ID : CVE-2023-6631**	N/A	A-SUB-POWE-290124/612
Vendor: sumanbhattarai					
Product: send_users_email					
Affected Version(s): * Up to (including) 1.4.3					
N/A	05-Jan-2024	5.3	Exposure of Sensitive Information to an Unauthorized	N/A	A-SUM-SEND-290124/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Actor vulnerability in Suman Bhattarai Send Users Email.This issue affects Send Users Email: from n/a through 1.4.3. **CVE ID : CVE-2023-52126**		
Vendor: surajghosh					
Product: hospital_management_system					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	9.8	A vulnerability classified as critical was found in Kashipara Hospital Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Parameter Handler. The manipulation of the argument email/password 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	N/A	A-SUR-HOSP-290124/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-249823. **CVE ID : CVE-2024-0267**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Kashipara Hospital Management System up to 1.0. Affected by this issue is some unknown functionality of the file registration.php. The manipulation of the argument name/email/pass/gender/age/city leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249824. **CVE ID : CVE-2024-0268**	N/A	A-SUR-HOSP-290124/615
Vendor: Svnlabs					
Product: html5_mp3_player_with_folder_feedburner_playlist_free					
Affected Version(s): * Up to (including) 2.8.0					
Deserialization of	08-Jan-2024	7.2	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares	N/A	A-SVN-HTML-290124/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			HTML5 MP3 Player with Folder Feedburner Playlist Free.This issue affects HTML5 MP3 Player with Folder Feedburner Playlist Free: from n/a through 2.8.0. **CVE ID : CVE-2023-52202**		
Product: html5_mp3_player_with_playlist_free					
Affected Version(s): * Up to (including) 3.0.0					
Deserialization of Untrusted Data	08-Jan-2024	8.8	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 MP3 Player with Playlist Free.This issue affects HTML5 MP3 Player with Playlist Free: from n/a through 3.0.0. **CVE ID : CVE-2023-52207**	N/A	A-SVN-HTML-290124/617
Product: html5_soundcloud_player_with_playlist_free					
Affected Version(s): * Up to (including) 2.8.0					
Deserialization of Untrusted Data	08-Jan-2024	7.2	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 SoundCloud Player with Playlist	N/A	A-SVN-HTML-290124/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Free.This issue affects HTML5 SoundCloud Player with Playlist Free: from n/a through 2.8.0. **CVE ID : CVE-2023-52205**		
Vendor: sygnoos					
Product: popup_builder					
Affected Version(s): * Up to (excluding) 4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Jan-2024	6.1	The Popup Builder WordPress plugin before 4.2.3 does not prevent simple visitors from updating existing popups, and injecting raw JavaScript in them, which could lead to Stored XSS attacks. **CVE ID : CVE-2023-6000**	N/A	A-SYG-POPU-290124/619
Vendor: synopsys					
Product: seeker					
Affected Version(s): * Up to (excluding) 2023.12.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	Synopsys Seeker versions prior to 2023.12.0 are vulnerable to a stored cross-site scripting vulnerability through a specially crafted payload.	N/A	A-SYN-SEEK-290124/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0226		
Vendor: taggbox					
Product: taggbox					
Affected Version(s): * Up to (including) 3.1					
Deserialization of Untrusted Data	08-Jan-2024	9.8	Deserialization of Untrusted Data vulnerability in Tagbox Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics.This issue affects Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics: from n/a through 3.1. **CVE ID : CVE-2023-52225**	N/A	A-TAG-TAGG-290124/621
Vendor: tasmoadmin					
Product: tasmoadmin					
Affected Version(s): * Up to (excluding) 3.3.0					
URL Redirection to Untrusted Site ('Open Redirect')	08-Jan-2024	6.1	Lack of "current" GET parameter validation during the action of changing a language leads to an open redirect vulnerability. **CVE ID : CVE-2023-6552**	https://github.com/TasmoAdmin/TasmoAdmin/pull/1039	A-TAS-TASM-290124/622
Vendor: teamwork_management_system_project					
Product: teamwork_management_system					
Affected Version(s): 2.28.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.1	Cross Site Scripting (XSS) vulnerability in xiweicheng TMS v.2.28.0 allows a remote attacker to execute arbitrary code via a crafted script to the click here function. **CVE ID : CVE-2023-50630**	N/A	A-TEA-TEAM-290124/623
Vendor: themeisle					
Product: rss_aggregator_by_feedzy					
Affected Version(s): * Up to (excluding) 4.3.3					
Missing Authorization	06-Jan-2024	5.4	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check when updating settings in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with author-level access or above to change the plugin's settings including proxy settings, which are also exposed to authors.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3012392%40feedzy-rss-feeds%2Ftrunk&old=2991547%40feedzy-rss-feeds%2Ftrunk&sfp_email=&sfph_mail=	A-THE-RSS_-290124/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6798		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Jan-2024	5.4	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6801**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3012392%40feedzy-rss-feeds%2Ftrunk&old=2991547%40feedzy-rss-feeds%2Ftrunk&sfp_email=&sfph_mail=	A-THE-RSS_-290124/625
Vendor: Themepunch					
Product: slider_revolution					
Affected Version(s): * Up to (excluding) 6.6.19					
Deserialization of Untrusted Data	08-Jan-2024	8.8	The Slider Revolution WordPress plugin before 6.6.19 does not prevent users	N/A	A-THE-SLID-290124/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with at least the Author role from unserializing arbitrary content when importing sliders, potentially leading to Remote Code Execution. **CVE ID : CVE-2023-6528**		
Vendor: themeum					
Product: wp_crowdfunding					
Affected Version(s): * Up to (excluding) 2.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	The WP Crowdfunding WordPress plugin before 2.1.9 does not sanitise and escape a parameter 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-2023-6161**	N/A	A-THE-WP_C-290124/627
Vendor: theresehansen					
Product: commenttweets					
Affected Version(s): * Up to (including) 0.6					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	The CommentTweets WordPress plugin through 0.6 does not have CSRF checks in some places, which could allow attackers to	N/A	A-THE-COMM-290124/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make logged in users perform unwanted actions via CSRF attacks **CVE ID : CVE-2023-6845**		
Vendor: tinowagner					
Product: jupyter_notebook_viewer					
Affected Version(s): * Up to (excluding) 0.1.6					
N/A	05-Jan-2024	9.8	nbviewer-app (aka Jupyter Notebook Viewer) before 0.1.6 has the get-task-allow entitlement for release builds. **CVE ID : CVE-2023-51277**	https://github.com/tuxu/nbviewer-app/commit/dc1e4ddf64c78e13175a39b076fa0646fc62e581	A-TIN-JUPY-290124/629
Vendor: tiny					
Product: tinymce					
Affected Version(s): * Up to (excluding) 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	TinyMCE versions before 5.10.0 are affected by a cross-site scripting vulnerability. A remote and unauthenticated attacker could introduce crafted image or link URLs that would result in the execution of arbitrary JavaScript in an editing user's browser. **CVE ID : CVE-2024-21910**	N/A	A-TIN-TINY-290124/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	TinyMCE versions before 5.6.0 are affected by a stored cross-site scripting vulnerability. An unauthenticated and remote attacker could insert crafted HTML into the editor resulting in arbitrary JavaScript execution in another user's browser. **CVE ID : CVE-2024-21911**	N/A	A-TIN-TINY-290124/631
Affected Version(s): * Up to (excluding) 5.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	TinyMCE versions before 5.9.0 are affected by a stored cross-site scripting vulnerability. An unauthenticated and remote attacker could insert crafted HTML into the editor resulting in arbitrary JavaScript execution in another user's browser.	N/A	A-TIN-TINY-290124/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21908		
Vendor: tonybybell					
Product: gtkwave					
Affected Version(s): 3.3.115					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `LZ4_decompress_safe_partial`. **CVE ID : CVE-2023-35955**	N/A	A-TON-GTKW-290124/633
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code	N/A	A-TON-GTKW-290124/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `fastlz_decompress`. **CVE ID : CVE-2023-35956**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `uncompress`. **CVE ID : CVE-2023-35957**	N/A	A-TON-GTKW-290124/635
Improper Restriction of Operations within the Bounds of	08-Jan-2024	7.8	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlock	N/A	A-TON-GTKW-290124/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			s2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the copy function `fstFread`. **CVE ID : CVE-2023-35958**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns `.ghw` decompression. **CVE ID : CVE-2023-35959**	N/A	A-TON-GTKW-290124/637
Improper Neutralization of Special Elements used in an	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the decompression functionality of	N/A	A-TON-GTKW-290124/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns legacy decompression in `vcd_main`. **CVE ID : CVE-2023-35960**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in `vcd_recorder_main`. **CVE ID : CVE-2023-35961**	N/A	A-TON-GTKW-290124/639
Improper Neutralization of Special	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the	N/A	A-TON-GTKW-290124/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2vzt` utility. **CVE ID : CVE-2023-35962**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt2` utility. **CVE ID : CVE-2023-35963**	N/A	A-TON-GTKW-290124/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	7.8	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt` utility. **CVE ID : CVE-2023-35964**	N/A	A-TON-GTKW-290124/642
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table` array.	N/A	A-TON-GTKW-290124/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36915		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table_lengths` array. **CVE ID : CVE-2023-36916**	N/A	A-TON-GTKW-290124/644
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability	N/A	A-TON-GTKW-290124/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concerns the out-of-bounds write when triggered via the GUI's legacy VCD parsing code. **CVE ID : CVE-2023-37416**		
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the GUI's interactive VCD parsing code. **CVE ID : CVE-2023-37417**	N/A	A-TON-GTKW-290124/646
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code	N/A	A-TON-GTKW-290124/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility. **CVE ID : CVE-2023-37418**		
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility. **CVE ID : CVE-2023-37419**	N/A	A-TON-GTKW-290124/648
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump	N/A	A-TON-GTKW-290124/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility. **CVE ID : CVE-2023-37420**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's default VCD parsing code. **CVE ID : CVE-2023-37442**	N/A	A-TON-GTKW-290124/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's legacy VCD parsing code. **CVE ID : CVE-2023-37443**	N/A	A-TON-GTKW-290124/651
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's	N/A	A-TON-GTKW-290124/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interactive VCD parsing code. **CVE ID : CVE-2023-37444**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility. **CVE ID : CVE-2023-37445**	N/A	A-TON-GTKW-290124/653
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability	N/A	A-TON-GTKW-290124/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility. **CVE ID : CVE-2023-37446**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility. **CVE ID : CVE-2023-37447**	N/A	A-TON-GTKW-290124/655
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious	N/A	A-TON-GTKW-290124/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's recoder (default) VCD parsing code. **CVE ID : CVE-2023-37573**		
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's legacy VCD parsing code. **CVE ID : CVE-2023-37574**	N/A	A-TON-GTKW-290124/657
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to	N/A	A-TON-GTKW-290124/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's interactive VCD parsing code. **CVE ID : CVE-2023-37575**		
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2vzt conversion utility. **CVE ID : CVE-2023-37576**	N/A	A-TON-GTKW-290124/659
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of	N/A	A-TON-GTKW-290124/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt2 conversion utility. **CVE ID : CVE-2023-37577**		
Use After Free	08-Jan-2024	7.8	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt conversion utility. **CVE ID : CVE-2023-37578**	N/A	A-TON-GTKW-290124/661
N/A	08-Jan-2024	7.8	Multiple arbitrary write vulnerabilities	N/A	A-TON-GTKW-290124/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2vzt conversion utility. **CVE ID : CVE-2023-37921**		
N/A	08-Jan-2024	7.8	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt2 conversion utility. **CVE ID : CVE-2023-37922**	N/A	A-TON-GTKW-290124/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jan-2024	7.8	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt conversion utility. **CVE ID : CVE-2023-37923**	N/A	A-TON-GTKW-290124/664
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow	N/A	A-TON-GTKW-290124/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when allocating the `rows` array. **CVE ID : CVE-2023-38618**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array. **CVE ID : CVE-2023-38619**	N/A	A-TON-GTKW-290124/666
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This	N/A	A-TON-GTKW-290124/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability concerns the integer overflow when allocating the `lsb` array. **CVE ID : CVE-2023-38620**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array. **CVE ID : CVE-2023-38621**	N/A	A-TON-GTKW-290124/668
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to	N/A	A-TON-GTKW-290124/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array. **CVE ID : CVE-2023-38622**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `vindex_offset` array. **CVE ID : CVE-2023-38623**	N/A	A-TON-GTKW-290124/670
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted	N/A	A-TON-GTKW-290124/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop. **CVE ID : CVE-2023-38648**		
Out-of-bounds Write	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the string copy loop. **CVE ID : CVE-2023-38649**	N/A	A-TON-GTKW-290124/672
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times	N/A	A-TON-GTKW-290124/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero. **CVE ID : CVE-2023-38650**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is zero.	N/A	A-TON-GTKW-290124/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38651		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero. **CVE ID : CVE-2023-38652**	N/A	A-TON-GTKW-290124/675
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability	N/A	A-TON-GTKW-290124/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concerns the integer overflow when num_time_ticks is zero. **CVE ID : CVE-2023-38653**		
Improper Validation of Array Index	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->numrealfacs`. **CVE ID : CVE-2023-39234**	N/A	A-TON-GTKW-290124/677
Improper Validation of Array Index	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to	N/A	A-TON-GTKW-290124/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->num_time_ticks`. **CVE ID : CVE-2023-39235**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `rows` array. **CVE ID : CVE-2023-39270**	N/A	A-TON-GTKW-290124/679
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted	N/A	A-TON-GTKW-290124/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array. **CVE ID : CVE-2023-39271**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `lsb` array. **CVE ID : CVE-2023-39272**	N/A	A-TON-GTKW-290124/681
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing	N/A	A-TON-GTKW-290124/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array. **CVE ID : CVE-2023-39273**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array. **CVE ID : CVE-2023-39274**	N/A	A-TON-GTKW-290124/683
Integer Overflow or	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities	N/A	A-TON-GTKW-290124/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `value` array. **CVE ID : CVE-2023-39275**		
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_pointers` array. **CVE ID : CVE-2023-39316**	N/A	A-TON-GTKW-290124/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	08-Jan-2024	7.8	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_lens` array. **CVE ID : CVE-2023-39317**	N/A	A-TON-GTKW-290124/686
Integer Underflow (Wrap or Wraparound)	08-Jan-2024	7.8	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing	N/A	A-TON-GTKW-290124/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the left shift operation. **CVE ID : CVE-2023-39413**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop. **CVE ID : CVE-2023-39443**	N/A	A-TON-GTKW-290124/688
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Jan-2024	7.8	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-	N/A	A-TON-GTKW-290124/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-bounds write perfomed by the string copy loop. **CVE ID : CVE-2023-39444**		
Integer Underflow (Wrap or Wraparound)	08-Jan-2024	7.3	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing the right shift operation. **CVE ID : CVE-2023-39414**	N/A	A-TON-GTKW-290124/690
Vendor: topazevolution					
Product: antifraud					
Affected Version(s): * Up to (including) 2.0.0.0					
N/A	08-Jan-2024	6.5	The wsftprm.sys kernel driver 2.0.0.0 in Topaz Antifraud allows low-privileged attackers to kill any (Protected Process Light) process via an IOCTL (which	N/A	A-TOP-ANTI-290124/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be named at a later time). **CVE ID : CVE-2023-52271**		
Vendor: Tp-link					
Product: tapo					
Affected Version(s): * Up to (excluding) 2.11.44					
Cleartext Storage of Sensitive Information	09-Jan-2024	7.5	TP-Link Tapo APK up to v2.12.703 uses hardcoded credentials for access to the login panel. **CVE ID : CVE-2023-27098**	N/A	A-TP--TAPO-290124/692
Vendor: trellix					
Product: agent					
Affected Version(s): * Up to (excluding) 5.8.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Jan-2024	7.8	A buffer overflow vulnerability in TA for Linux and TA for MacOS prior to 5.8.1 allows a local user to gain elevated permissions, or cause a Denial of Service (DoS), through exploiting a memory corruption issue in the TA service, which runs as root. This may also result in the disabling of event reporting to ePO, caused by failure to	https://kcm.trellix.com/corporate/index?page=content&id=SB10416	A-TRE-AGEN-290124/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate input from the file correctly. **CVE ID : CVE-2024-0213**		
Vendor: ukrsolution					
Product: simple_inventory_management					
Affected Version(s): * Up to (including) 1.5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UkrSolution Simple Inventory Management – just scan barcode to manage products and orders. For WooCommerce.This issue affects Simple Inventory Management – just scan barcode to manage products and orders. For WooCommerce: from n/a through 1.5.1. **CVE ID : CVE-2023-52215**	N/A	A-UKR-SIMP-290124/694
Vendor: uncannyowl					
Product: uncanny_automator					
Affected Version(s): * Up to (including) 5.1.0.2					
N/A	05-Jan-2024	5.3	Exposure of Sensitive Information to an	N/A	A-UNC-UNCA-290124/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unauthorized Actor vulnerability in Uncanny Automator, Uncanny Owl Uncanny Automator – Automate everything with the #1 no-code automation and integration plugin.This issue affects Uncanny Automator – Automate everything with the #1 no-code automation and integration plugin: from n/a through 5.1.0.2. **CVE ID : CVE-2023-52151**		
Vendor: ureport2_project					
Product: ureport2					
Affected Version(s): * Up to (including) 2.2.9					
N/A	03-Jan-2024	9.8	Arbitrary File Write vulnerability in the saveReportFile method of ureport2 2.2.9 and before allows attackers to write arbitrary files and run arbitrary commands via crafted POST request. **CVE ID : CVE-2023-50090**	N/A	A-URE-UREP-300124/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: vapor					
Product: vapor					
Affected Version(s): * Up to (excluding) 4.90.0					
Integer Overflow or Wraparound	03-Jan-2024	6.5	Vapor is an HTTP web framework for Swift. Prior to version 4.90.0, Vapor's `vapor_urlparser_parse` function uses `uint16_t` indexes when parsing a URI's components, which may cause integer overflows when parsing untrusted inputs. This vulnerability does not affect Vapor directly but could impact applications relying on the URI type for validating user input. The URI type is used in several places in Vapor. A developer may decide to use URI to represent a URL in their application (especially if that URL is then passed to the HTTP Client) and rely on its public properties and methods. However, URI may fail to properly parse a valid (albeit abnormally long) URL, due to	https://github.com/vapor/vapor/commit/6db3d917b5ce5024a84eb265ef65691383305d70, https://github.com/vapor/vapor/security/advisories/GHSA-r6r4-5pr8-gjcp	A-VAP-VAPO-300124/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			string ranges being converted to 16-bit integers. An attacker may use this behavior to trick the application into accepting a URL to an untrusted destination. By padding the port number with zeros, an attacker can cause an integer overflow to occur when the URL authority is parsed and, as a result, spoof the host. Version 4.90.0 contains a patch for this issue. As a workaround, validate user input before parsing as a URI or, if possible, use Foundation's `URL` and `URLComponents` utilities. **CVE ID : CVE-2024-21631**		
Vendor: veronalabs					
Product: wp_sms					
Affected Version(s): * Up to (excluding) 6.5.1					
Improper Neutralization of Special Elements used in an SQL	03-Jan-2024	4.9	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for	https://github.com/wp-sms/wp-sms/commit/6656de201efe67c7983102c344a546eed976a819	A-VER-WP_S-300124/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			WordPress is vulnerable to SQL Injection via the 'group_id' parameter in all versions up to, and including, 6.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can leveraged to achieve Reflected Cross-site Scripting. **CVE ID : CVE-2023-6981**	, https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3015006%40wp-sms&new=3015006%40wp-sms&sfp_email=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation	03-Jan-2024	4.3	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for WordPress is	https://github.com/wp-sms/wp-sms/commit/0f36e2f521ade8ddfb3e04786defe074370afb50, https://plugins.	A-VER-WP_S-300124/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.5. This is due to missing or incorrect nonce validation on the 'delete' action of the wp-sms-subscribers page. This makes it possible for unauthenticated attackers to delete subscribers via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-6980**	trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3015006%40wp-sms&new=3015006%40wp-sms&sfp_email=&sfph_mail=	
Vendor: verot					
Product: class.upload.php					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	04-Jan-2024	5.4	As a simple library, class.upload.php does not perform an in-depth check on uploaded files, allowing a stored XSS vulnerability when the default configuration is used. Developers must be aware of that fact and use extension	N/A	A-VER-CLAS-300124/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whitelisting accompanied by forcing the server to always provide content-type based on the file extension. The README has been updated to include these guidelines. **CVE ID : CVE-2023-6551**		
Vendor: Videowhisper					
Product: rate_star_review					
Affected Version(s): * Up to (including) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Jan-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VideoWhisper Rate Star Review – AJAX Reviews for Content, with Star Ratings allows Reflected XSS.This issue affects Rate Star Review – AJAX Reviews for Content, with Star Ratings: from n/a through 1.5.1.	N/A	A-VID-RATE-300124/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52213		
Vendor: viewcomponent					
Product: view_component					
Affected Version(s): * Up to (excluding) 2.83.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.1	view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. Versions prior to 3.9.0 and 2.83.0 have a cross-site scripting vulnerability that has the potential to impact anyone rendering a component directly from a controller with the view_component gem. Note that only components that define a `#call` method (i.e. instead of using a sidecar template) are affected. The return value of the `#call` method is not sanitized and can include user-defined content. In addition, the return value of the `#output_postamble` methodis not	https://github.com/ViewComponent/view_component/commit/0d26944a8d2730ea40e60eae23d70684483e5017, https://github.com/ViewComponent/view_component/commit/c43d8bafa7117cbce479669a423ab266de150697, https://github.com/ViewComponent/view_component/pull/1950	A-VIE-VIEW-300124/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitized, which can also lead to cross-site scripting issues. Versions 3.9.0 and 2.83.0 have been released and fully mitigate both the `#call` and the `#output_postamble` vulnerabilities. As a workaround, sanitize the return value of `#call`. **CVE ID : CVE-2024-21636**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	6.1	view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. Versions prior to 3.9.0 and 2.83.0 have a cross-site scripting vulnerability that has the potential to impact anyone rendering a component directly from a controller with the view_component gem. Note that only components that define a `#call` method (i.e. instead of using a sidecar template) are affected. The	https://github.com/ViewComponent/view_component/commit/0d26944a8d2730ea40e60eae23d70684483e5017, https://github.com/ViewComponent/view_component/commit/c43d8bafa7117cbce479669a423ab266de150697, https://github.com/ViewComponent/view_component/pull/1950	A-VIE-VIEW-300124/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			return value of the `#call` method is not sanitized and can include user-defined content. In addition, the return value of the `#output_postamble` methodis not sanitized, which can also lead to cross-site scripting issues. Versions 3.9.0 and 2.83.0 have been released and fully mitigate both the `#call` and the `#output_postamble` vulnerabilities. As a workaround, sanitize the return value of `#call`. **CVE ID : CVE-2024-21636**		
Vendor: wallix					
Product: bastion					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.6					
N/A	08-Jan-2024	7.5	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure. **CVE ID : CVE-2023-49961**	https://www.wallix.com/support/alerts/	A-WAL-BAST-300124/704
Affected Version(s): From (including) 10.4.0 Up to (excluding) 10.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Jan-2024	7.5	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure. **CVE ID : CVE-2023-49961**	https://www.wallix.com/support/alerts/	A-WAL-BAST-300124/705
Affected Version(s): From (including) 7.0.0 Up to (excluding) 9.0.10					
N/A	08-Jan-2024	7.5	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure. **CVE ID : CVE-2023-49961**	https://www.wallix.com/support/alerts/	A-WAL-BAST-300124/706
Product: bastion_access_manager					
Affected Version(s): From (including) 3.0.0 Up to (including) 4.0.3					
N/A	08-Jan-2024	7.5	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure. **CVE ID : CVE-2023-49961**	https://www.wallix.com/support/alerts/	A-WAL-BAST-300124/707
Vendor: webcodingplace					
Product: product_expiry_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	03-Jan-2024	4.3	The Product Expiry for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_settings' function in versions up to, and including, 2.5. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update plugin settings. **CVE ID : CVE-2024-0201**	N/A	A-WEB-PROD-300124/708
Vendor: webtoffee					
Product: woocommerce_pdf_invoices\,_packing_slips\,_delivery_notes_and_shipping_labels					
Affected Version(s): * Up to (excluding) 4.3.1					
Missing Authorization	03-Jan-2024	6.5	The WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on theprint_packinglist action in all	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3014977%40print-invoices-packing-slip-labels-for-woocommerce&new=3014977%40print-invoices-packing-slip-	A-WEB-WOOC-300124/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 4.3.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to export orders which can contain sensitive information. **CVE ID : CVE-2023-7068**	labels-for-woocommerce&sfp_email=&sfph_mail=	
Vendor: wedevs					
Product: wp_erp					
Affected Version(s): * Up to (excluding) 1.12.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Jan-2024	4.9	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting.This issue affects WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting: from n/a through 1.12.8.	N/A	A-WED-WP_E-300124/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21747		
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): 4.2.0					
Out-of-bounds Read	03-Jan-2024	7.5	HTTP3 dissector crash in Wireshark 4.2.0 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0207**	https://gitlab.com/wireshark/wireshark/-/issues/19502, https://www.wireshark.org/security/wnpa-sec-2024-03.html	A-WIR-WIRE-300124/711
Uncontrolled Recursion	03-Jan-2024	7.5	GVCP dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0208**	https://gitlab.com/wireshark/wireshark/-/issues/19496, https://www.wireshark.org/security/wnpa-sec-2024-01.html	A-WIR-WIRE-300124/712
NULL Pointer Dereference	03-Jan-2024	7.5	IEEE 1609.2 dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0209**	https://gitlab.com/wireshark/wireshark/-/issues/19501, https://www.wireshark.org/security/wnpa-sec-2024-02.html	A-WIR-WIRE-300124/713
Uncontrolled Recursion	03-Jan-2024	7.5	Zigbee TLV dissector crash in Wireshark 4.2.0 allows denial of service via packet	https://gitlab.com/wireshark/wireshark/-/issues/19504, https://www.w	A-WIR-WIRE-300124/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection or crafted capture file **CVE ID : CVE-2024-0210**	ireshark.org/security/wnpa-sec-2024-04.html	
Uncontrolled Recursion	03-Jan-2024	7.5	DOCSIS dissector crash in Wireshark 4.2.0 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0211**	https://gitlab.com/wireshark/wireshark/-/issues/19557, https://www.wireshark.org/security/wnpa-sec-2024-05.html	A-WIR-WIRE-300124/715
Affected Version(s): From (including) 3.6.0 Up to (including) 3.6.19					
Uncontrolled Recursion	03-Jan-2024	7.5	GVCP dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0208**	https://gitlab.com/wireshark/wireshark/-/issues/19496, https://www.wireshark.org/security/wnpa-sec-2024-01.html	A-WIR-WIRE-300124/716
NULL Pointer Dereference	03-Jan-2024	7.5	IEEE 1609.2 dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0209**	https://gitlab.com/wireshark/wireshark/-/issues/19501, https://www.wireshark.org/security/wnpa-sec-2024-02.html	A-WIR-WIRE-300124/717
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.11					
Uncontrolled Recursion	03-Jan-2024	7.5	GVCP dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to	https://gitlab.com/wireshark/wireshark/-/issues/19496,	A-WIR-WIRE-300124/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0208**	https://www.wireshark.org/security/wnpa-sec-2024-01.html	
NULL Pointer Dereference	03-Jan-2024	7.5	IEEE 1609.2 dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2024-0209**	https://gitlab.com/wireshark/wireshark/-/issues/19501, https://www.wireshark.org/security/wnpa-sec-2024-02.html	A-WIR-WIRE-300124/719
Vendor: wiselyhub					
Product: js_help_desk					
Affected Version(s): * Up to (including) 2.7.1					
Unrestricted Upload of File with Dangerous Type	05-Jan-2024	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.7.1. **CVE ID : CVE-2022-46839**	N/A	A-WIS-JS_H-300124/720
Vendor: Woocommerce					
Product: woocommerce					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 8.2.2					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Automattic WooCommerce.This issue affects WooCommerce: from n/a through 8.2.2. **CVE ID : CVE-2023-52222**	N/A	A-WOO-WOOC-300124/721
Vendor: wow-company					
Product: floating_button					
Affected Version(s): * Up to (including) 6.0					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Floating Button.This issue affects Floating Button: from n/a through 6.0. **CVE ID : CVE-2023-52149**	N/A	A-WOW-FLOA-300124/722
Vendor: wp-blogs-planetarium_project					
Product: wp-blogs-planetarium					
Affected Version(s): * Up to (including) 1.0					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	The WP Blogs' Planetarium WordPress plugin through 1.0 does not have CSRF check in place	N/A	A-WP--WP-B-300124/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2023-6532**		
Vendor: wp-members_project					
Product: wp-members					
Affected Version(s): * Up to (including) 3.4.8					
Missing Authorization	04-Jan-2024	6.5	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.4.8 via the wpmem_field shortcode. This makes it possible for authenticated attackers, with contributor access and above, to extract sensitive data including user emails, password hashes, usernames, and more. **CVE ID : CVE-2023-6733**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3015224%40wp-members%2Ftrunk&old=2920897%40wp-members%2Ftrunk&sfp_email=&sfph_mail=	A-WP--WP-M-300124/724
Vendor: wp-staging					
Product: wp_staging					
Affected Version(s): * Up to (excluding) 3.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Jan-2024	7.5	The WP STAGING WordPress Backup Plugin before 3.1.3 and WP STAGING Pro WordPress Backup Plugin before 5.1.3 do not prevent visitors from leaking key information about ongoing backups processes, allowing unauthenticated attackers to download said backups later. **CVE ID : CVE-2023-6113**	N/A	A-WP--WP_S-300124/725
Vendor: wpaffiliatemanager					
Product: affiliates_manager					
Affected Version(s): * Up to (including) 2.9.30					
N/A	05-Jan-2024	5.3	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.30. **CVE ID : CVE-2023-52148**	N/A	A-WPA-AFFI-300124/726
Affected Version(s): * Up to (including) 2.9.31					
Cross-Site Request	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in	N/A	A-WPA-AFFI-300124/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.31. **CVE ID : CVE-2023-52130**		
Vendor: wpchill					
Product: download_monitor					
Affected Version(s): * Up to (including) 4.7.60					
N/A	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPChill Download Monitor.This issue affects Download Monitor: from n/a through 4.7.60. **CVE ID : CVE-2022-45354**	N/A	A-WPC-DOWN-300124/728
Vendor: wpclever					
Product: wpc_product_bundles_for_woocommerce					
Affected Version(s): * Up to (including) 7.3.1					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WPClever WPC Product Bundles for WooCommerce.Thi	N/A	A-WPC-WPC_-300124/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s issue affects WPC Product Bundles for WooCommerce: from n/a through 7.3.1. **CVE ID : CVE-2023-52127**		
Vendor: wpdeveloper					
Product: embedpress					
Affected Version(s): * Up to (excluding) 3.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	5.4	The EmbedPress – Embed PDF, YouTube, Google Docs, Vimeo, Wistia Videos, Audios, Maps & Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's embed_oembed_html shortcode in all versions up to 3.9.5 (exclusive) 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	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3014595%40embedpress&new=3014595%40embedpress&sfp_email=&sfph_mail=#file11	A-WPD-EMBE-300124/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6986**		
Product: essential_addons_for_elementor					
Affected Version(s): * Up to (including) 5.9.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Jan-2024	5.4	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom ID in all versions up to, and including, 5.9.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access and higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-7044**	https://plugins.trac.wordpress.org/browser/essential-addons-for-elementor-lite/trunk/includes/Extensions/Wrapper_Link.php#L65	A-WPD-ESSE-300124/731
Vendor: wpdownloadmanager					
Product: wordpress_download_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.2.83					
Insufficiently Protected Credentials	01-Jan-2024	7.5	The Download Manager WordPress plugin before 3.2.83 does not protect file download's passwords, leaking it upon receiving an invalid one. **CVE ID : CVE-2023-6421**	N/A	A-WPD-WORD-300124/732
Vendor: wpexperts					
Product: post_smtp					
Affected Version(s): * Up to (excluding) 2.8.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'msg' parameter in all versions up to, and including, 2.8.6 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	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3012318%40post-smtp%2Ftrunk&old=3006604%40post-smtp%2Ftrunk&sfp_email=&sfph_mail=#file4	A-WPE-POST-300124/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID : CVE-2023-6629**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	6.1	The POST SMTP WordPress plugin before 2.8.7 does not sanitise and escape the msg parameter 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-2023-6621**	N/A	A-WPE-POST-300124/734
Affected Version(s): * Up to (excluding) 2.8.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	5.4	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'device' header in all versions up to, and including, 2.8.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3016126%40post-smtp%2Ftrunk&old=3012318%40post-smtp%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-POST-300124/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-7027**		
Vendor: wpjobportal					
Product: wp_job_portal					
Affected Version(s): * Up to (including) 2.0.6					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Job Portal WP Job Portal – A Complete Job Board.This issue affects WP Job Portal – A Complete Job Board: from n/a through 2.0.6. **CVE ID : CVE-2023-52184**	N/A	A-WPJ-WP_J-300124/736
Vendor: wpmet					
Product: metform_elementor_contact_form_builder					
Affected Version(s): * Up to (including) 3.8.1					
Cross-Site Request Forgery (CSRF)	09-Jan-2024	5.4	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and	https://plugins.trac.wordpress.org/browser/metform/trunk/core/integrations/crm/hubspot/loader.php#L87, https://plugins.	A-WPM-METF-300124/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 3.8.1. This is due to missing or incorrect nonce validation on the contents function. This makes it possible for unauthenticated attackers to update the options "mf_hubsopt_token", "mf_hubsopt_refresh_token", "mf_hubsopt_token_type", and "mf_hubsopt_expires_in" via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This would allow an attacker to connect their own Hubspot account to a victim site's metform to obtain leads and contacts. **CVE ID : CVE-2023-6788**	trac.wordpress.org/changeset/3011284/metform/trunk/core/integrations/crm/hubspot/loader.php	
Vendor: wpmudev					
Product: defender_security					
Affected Version(s): * Up to (including) 4.1.0					
Insertion of Sensitive Information into Log File	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability	N/A	A-WPM-DEFE-300124/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in WPMU DEV Defender Security – Malware Scanner, Login Security & Firewall.This issue affects Defender Security – Malware Scanner, Login Security & Firewall: from n/a through 4.1.0. **CVE ID : CVE-2023-51490**		
Vendor: wpswings					
Product: coupon_referral_program					
Affected Version(s): * Up to (including) 1.7.2					
N/A	08-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Swings Coupon Referral Program.This issue affects Coupon Referral Program: from n/a through 1.7.2. **CVE ID : CVE-2023-52190**	N/A	A-WPS-COUP-300124/739
Vendor: wpzone					
Product: inline_image_upload_for_bbpress					
Affected Version(s): * Up to (including) 1.1.18					
Cross-Site Request Forgery (CSRF)	05-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Zone Inline Image Upload for	N/A	A-WPZ-INLI-300124/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BBPress.This issue affects Inline Image Upload for BBPress: from n/a through 1.1.18. **CVE ID : CVE-2023-51668**		
Vendor: Xwiki					
Product: Xwiki					
Affected Version(s): * Up to (excluding) 14.10.17					
Improper Control of Generation of Code ('Code Injection')	08-Jan-2024	9.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to a remote code execution (RCE) attack through its user registration feature. This issue allows an attacker to execute arbitrary code by crafting malicious payloads in the "first name" or "last name" fields during user registration. This impacts all installations that have user registration enabled for guests. This vulnerability has been patched in XWiki 14.10.17,	https://github.com/xwiki/xwiki-platform/commit/b290bfd573c6f7db6cc15a88dd4111d9fcad0d31, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rj7p-xjv7-7229, https://jira.xwiki.org/browse/XWIKI-21173	A-XWI-XWIK-300124/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21650**		
Improper Handling of Insufficient Privileges	09-Jan-2024	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The rollback action is missing a right protection, a user can rollback to a previous version of the page to gain rights they don't have anymore. The problem has been patched in XWiki 14.10.17, 15.5.3 and 15.8-rc-1 by ensuring that the rights are checked before performing the rollback. **CVE ID : CVE-2024-21648**	https://github.com/xwiki/xwiki-platform/commit/4de72875ca4960279616542741033bfdbf1e680, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-xh35-w7wg-95v3, https://jira.xwiki.org/browse/XWIKI-21257	A-XWI-XWIK-300124/742
Affected Version(s): From (including) 14.10 Up to (excluding) 14.10.18					
Uncontrolled Resource Consumption	09-Jan-2024	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user able to attach a file to a page can post a malformed TAR file by manipulating file modification times headers, which	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-8959-rfxh-r4j4, https://jira.xwiki.org/browse/XCOMMONS-2796	A-XWI-XWIK-300124/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when parsed by Tika, could cause a denial of service issue via CPU consumption. This vulnerability has been patched in XWiki 14.10.18, 15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21651**		
Affected Version(s): From (including) 15.0 Up to (excluding) 15.5.3					
Improper Control of Generation of Code ('Code Injection')	08-Jan-2024	9.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to a remote code execution (RCE) attack through its user registration feature. This issue allows an attacker to execute arbitrary code by crafting malicious payloads in the "first name" or "last name" fields during user registration. This impacts all installations that have user registration enabled for guests. This vulnerability has been patched in XWiki 14.10.17,	https://github.com/xwiki/xwiki-platform/commit/b290bfd573c6f7db6cc15a88dd4111d9fcad0d31, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rj7p-xjv7-7229, https://jira.xwiki.org/browse/XWIKI-21173	A-XWI-XWIK-300124/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21650**		
Improper Handling of Insufficient Privileges	09-Jan-2024	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The rollback action is missing a right protection, a user can rollback to a previous version of the page to gain rights they don't have anymore. The problem has been patched in XWiki 14.10.17, 15.5.3 and 15.8-rc-1 by ensuring that the rights are checked before performing the rollback. **CVE ID : CVE-2024-21648**	https://github.com/xwiki/xwiki-platform/commit/4de72875ca4960279616542741033bfdbf1e680, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-xh35-w7wg-95v3, https://jira.xwiki.org/browse/XWIKI-21257	A-XWI-XWIK-300124/745
Affected Version(s): From (including) 15.5 Up to (excluding) 15.5.3					
Uncontrolled Resource Consumption	09-Jan-2024	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user able to attach a file to a page can post a malformed TAR file by manipulating file modification times headers, which	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-8959-rfxh-r4j4, https://jira.xwiki.org/browse/XCOMMONS-2796	A-XWI-XWIK-300124/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when parsed by Tika, could cause a denial of service issue via CPU consumption. This vulnerability has been patched in XWiki 14.10.18, 15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21651**		
Affected Version(s): From (including) 15.6 Up to (excluding) 15.8					
Improper Handling of Insufficient Privileges	09-Jan-2024	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The rollback action is missing a right protection, a user can rollback to a previous version of the page to gain rights they don't have anymore. The problem has been patched in XWiki 14.10.17, 15.5.3 and 15.8-rc-1 by ensuring that the rights are checked before performing the rollback. **CVE ID : CVE-2024-21648**	https://github.com/xwiki/xwiki-platform/commit/4de72875ca4960279616542741033bfdbf1e680, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-xh35-w7wg-95v3, https://jira.xwiki.org/browse/XWIKI-21257	A-XWI-XWIK-300124/747
Uncontrolled Resource	09-Jan-2024	6.5	XWiki Platform is a generic wiki platform offering runtime services	https://github.com/xwiki/xwiki-platform/securi	A-XWI-XWIK-300124/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			for applications built on top of it. A user able to attach a file to a page can post a malformed TAR file by manipulating file modification times headers, which when parsed by Tika, could cause a denial of service issue via CPU consumption. This vulnerability has been patched in XWiki 14.10.18, 15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21651**	ty/advisories/GHSA-8959-rfxh-r4j4, https://jira.xwiki.org/browse/XCOMMONS-2796	
Affected Version(s): From (including) 15.6 Up to (including) 15.7					
Improper Control of Generation of Code ('Code Injection')	08-Jan-2024	9.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to a remote code execution (RCE) attack through its user registration feature. This issue allows an attacker to execute arbitrary code by crafting malicious payloads in the "first name" or "last name" fields during user	https://github.com/xwiki/xwiki-platform/commit/b290bfd573c6f7db6cc15a88dd4111d9fcad0d31, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rj7p-xjv7-7229, https://jira.xwiki.org/browse/XWIKI-21173	A-XWI-XWIK-300124/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration. This impacts all installations that have user registration enabled for guests. This vulnerability has been patched in XWiki 14.10.17, 15.5.3 and 15.8 RC1. **CVE ID : CVE-2024-21650**		
Vendor: yasm_project					
Product: yasm					
Affected Version(s): 1.3.0.86.g9def					
Use After Free	03-Jan-2024	5.5	Use After Free vulnerability in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the do_directive function in the modules/preprocs /nasm/nasm-pp.c component. **CVE ID : CVE-2023-49554**	https://github.com/yasm/yasm/issues/249	A-YAS-YASM-300124/750
N/A	03-Jan-2024	5.5	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expand_smacro function in the modules/preprocs /nasm/nasm-pp.c component.	https://github.com/yasm/yasm/issues/248	A-YAS-YASM-300124/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49555		
N/A	03-Jan-2024	5.5	Buffer Overflow vulnerability in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expr_delete_term function in the libyasm/expr.c component. **CVE ID : CVE-2023-49556**	https://github.com/yasm/yasm/issues/250	A-YAS-YASM-300124/752
N/A	03-Jan-2024	5.5	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the yasm_section_bcs_first function in the libyasm/section.c component. **CVE ID : CVE-2023-49557**	https://github.com/yasm/yasm/issues/253	A-YAS-YASM-300124/753
N/A	03-Jan-2024	5.5	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expand_mmac_params function in the modules/preprocs/nasm/nasm-pp.c component. **CVE ID : CVE-2023-49558**	https://github.com/yasm/yasm/issues/252	A-YAS-YASM-300124/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: yevhenkotelnytskyi					
Product: js_\&_css_script_optimizer					
Affected Version(s): * Up to (including) 0.3.3					
Cross-Site Request Forgery (CSRF)	08-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Yevhen Kotelnytskyi JS & CSS Script Optimizer.This issue affects JS & CSS Script Optimizer: from n/a through 0.3.3. **CVE ID : CVE-2023-52216**	N/A	A-YEV-JS_\-300124/755
Vendor: yogeshojha					
Product: rengine					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Jan-2024	8.8	reNgine through 2.0.2 allows OS Command Injection if an adversary has a valid session ID. The attack places shell metacharacters in an api/tools/waf_detector/?url= string. The commands are executed as root via subprocess.check_output. **CVE ID : CVE-2023-50094**	N/A	A-YOG-RENG-300124/756
Vendor: youke365					
Product: youke_365					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.5.0 Up to (including) 1.5.3					
Server-Side Request Forgery (SSRF)	08-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Youke365 up to 1.5.3. Affected is an unknown function of the file /app/api/controller/caiji.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249870 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0303**	N/A	A-YOU-YOUK-300124/757
Server-Side Request Forgery (SSRF)	08-Jan-2024	9.8	A vulnerability has been found in Youke365 up to 1.5.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /app/api/controller/collect.php. The manipulation of the	N/A	A-YOU-YOUK-300124/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument url leads to server-side request forgery. 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-249871. **CVE ID : CVE-2024-0304**		
Vendor: yugeshverma					
Product: online_lawyer_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Jan-2024	5.4	A vulnerability classified as problematic has been found in Project Worlds Online Lawyer Management System 1.0. Affected is an unknown function of the component User Registration. The manipulation of the argument First Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249822 is the identifier	N/A	A-YUG-ONLI-300124/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2024-0266**		
Vendor: Zimbra					
Product: zm-ajax					
Affected Version(s): * Up to (excluding) 8.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Jan-2024	4.7	A vulnerability has been found in Zimbra zm-ajax up to 8.8.1 and classified as problematic. Affected by this vulnerability is the function XFormItem.prototype.setError of the file WebRoot/js/ajax/dwt/xforms/XFormItem.js. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 8.8.2 is able to address this issue. The identifier of the patch is 8d039d6efe80780adc40c6f670c06d21de272105. It is	https://github.com/Zimbra/zm-ajax/commit/8d039d6efe80780adc40c6f670c06d21de272105	A-ZIM-ZM-A-300124/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended to upgrade the affected component. The identifier VDB-249421 was assigned to this vulnerability. **CVE ID : CVE-2017-20188**		
Vendor: Zohocorp					
Product: manageengine_firewall_analyzer					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/761
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**		
Product: manageengine_netflow_analyzer					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/763
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**		
Product: manageengine_network_configuration_manager					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/765
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to trigger this vulnerability. **CVE ID : CVE-2023-47211**		
Product: manageengine_opmanager					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/767
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability.	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47211		
Product: manageengine_opmanager_msp					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/769
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: manageengine_opmanager_plus					
Affected Version(s): * Up to (excluding) 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/771
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/772
Product: manageengine_oputils					
Affected Version(s): * Up to (excluding) 12.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/773
Affected Version(s): 12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2024	8.6	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability. **CVE ID : CVE-2023-47211**	https://www.manageengine.com/itom/advisory/cve-2023-47211.html	A-ZOH-MANA-300124/774
Hardware					
Vendor: autelrobotics					
Product: evo_nano_drone					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jan-2024	5.7	Autel EVO NANO drone flight control firmware version 1.6.5 is vulnerable to denial of service (DoS). **CVE ID : CVE-2023-50121**	N/A	H-AUT-EVO_-300124/775
Vendor: automaticsystems					
Product: soc_fl9600_firstlane					
Affected Version(s): -					
Use of Hard-coded Credentials	03-Jan-2024	7.5	An issue in Automatic Systems SOC FL9600 FastLine v.lego_T04E00 allows a remote attacker to obtain sensitive information via the admin login credentials. **CVE ID : CVE-2023-37608**	N/A	H-AUT-SOC_-300124/776
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Jan-2024	7.5	Directory Traversal in Automatic-Systems SOC FL9600 FastLine lego_T04E00 allows a remote attacker to obtain sensitive information. **CVE ID : CVE-2023-37607**	N/A	H-AUT-SOC_-300124/777
Vendor: byzoro					
Product: smart_s150					
Affected Version(s): -					
Unrestricted Upload of	08-Jan-2024	9.8	A vulnerability was found in Beijing	N/A	H-BYZ-SMAR-300124/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			Baichuo Smart S150 Management Platform up to 20240101. It has been rated as critical. Affected by this issue is some unknown functionality of the file /useratte/useratte station.php of the component HTTP POST Request Handler. The manipulation of the argument web_img leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249866 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-2024-0300**		
Vendor: Dlink					
Product: r15					
Affected Version(s): -					
N/A	10-Jan-2024	5.3	D-Link R15 before v1.08.02 was	https://support announcement.	H-DLI-R15-300124/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain no firewall restrictions for IPv6 traffic. This allows attackers to arbitrarily access any services running on the device that may be inadvertently listening via IPv6. **CVE ID : CVE-2023-41603**	us.dlink.com/announcement/publication.aspx?name=SAP10347	
Vendor: geniecompany					
Product: aladdin_connect_garage_door_opener					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	8.8	When the Genie Company Aladdin Connect garage door opener (Retrofit-Kit Model ALDCM) is placed into configuration mode the web servers “Garage Door Control Module Setup” page is vulnerable to XSS via a broadcast SSID name containing malicious code with client side Java Script and/or HTML. This allows the attacker to inject malicious code with client side Java Script and/or HTML into the	https://www.rapid7.com/blog/post/2024/01/03/genie-aladdin-connect-retrofit-garage-door-opener-multiple-vulnerabilities/	H-GEN-ALAD-300124/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users' web browser. **CVE ID : CVE-2023-5880**		
Missing Authentication for Critical Function	03-Jan-2024	8.2	Unauthenticated access permitted to web interface page The Genie Company Aladdin Connect (Retrofit-Kit Model ALDCM) "Garage Door Control Module Setup" and modify the Garage door's SSID settings. **CVE ID : CVE-2023-5881**	https://www.rapid7.com/blog/post/2024/01/03/genie-aladdin-connect-retrofit-garage-door-opener-multiple-vulnerabilities/	H-GEN-ALAD-300124/781
Vendor: gl-inet					
Product: gl-a1300					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7,	N/A	H-GL--GL-A-300124/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	H-GL--GL-A-300124/783
Product: gl-ar300m					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface	N/A	H-GL--GL-A-300124/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7,	N/A	H-GL--GL-A-300124/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-ar750					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	H-GL--GL-A-300124/786
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific	N/A	H-GL--GL-A-300124/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-ar750s					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	N/A	H-GL--GL-A-300124/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50921		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	H-GL--GL-A-300124/789
Product: gl-ax1800					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root	N/A	H-GL--GL-A-300124/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	N/A	H-GL--GL-A-300124/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50922		
Product: gl-axt1800					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	H-GL--GL-A-300124/792
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its	N/A	H-GL--GL-A-300124/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-b1300					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	H-GL--GL-B-300124/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	H-GL--GL-B-300124/795
Product: gl-mt1300					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6,	N/A	H-GL--GL-M-300124/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	H-GL--GL-M-300124/797
Product: gl-mt2500					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	H-GL--GL-M-300124/798
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6,	N/A	H-GL--GL-M-300124/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-mt3000					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	H-GL--GL-M-300124/800
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are	N/A	H-GL--GL-M-300124/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-mt300n-v2					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7,	N/A	H-GL--GL-M-300124/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	H-GL--GL-M-300124/803
Product: gl-mt6000					
Affected Version(s): -					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0.	N/A	H-GL--GL-M-300124/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7,	N/A	H-GL--GL-M-300124/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Vendor: Google					
Product: home					
Affected Version(s): -					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	H-GOO-HOME-300124/806
Product: home_mini					
Affected Version(s): -					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	H-GOO-HOME-300124/807
Product: nest_audio					
Affected Version(s): -					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on	https://support.google.com/product-documentation/	H-GOO-NEST-300124/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	
Product: nest_mini					
Affected Version(s): -					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	H-GOO-NEST-300124/809
Product: nest_wifi_pro					
Affected Version(s): -					
Missing Encryption of Sensitive Data	02-Jan-2024	9.8	Google Nest WiFi Pro root code-execution & user-data compromise **CVE ID : CVE-2023-6339**	N/A	H-GOO-NEST-300124/810
Product: pixel					
Affected Version(s): -					
Missing Authorization	02-Jan-2024	5.5	There is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of health data with no	https://source.android.com/docs/security/bulletin/pixel-watch/2023/2023-12-01	H-GOO-PIXE-300124/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2023-4164**		
Product: pixel_watch					
Affected Version(s): 11					
N/A	02-Jan-2024	7.8	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation **CVE ID : CVE-2023-48418**	https://source.android.com/docs/security/bulletin/pixel-watch/2023/2023-12-01	H-GOO-PIXE-300124/812
Vendor: hitachienergy					
Product: relion_650					
Affected Version(s): -					
Improper Verification of Cryptograp	04-Jan-2024	4.5	A vulnerability exists in the Relion update package	https://publisher.hitachienergy.com/preview?DocumentID=8	H-HIT-RELI-300124/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	
Product: relion_670					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPart	H-HIT-RELI-300124/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	Id=&Action=Launch	
Product: relion_sam600-io					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RELI-300124/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Product: rtu520					
Affected Version(s): -					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RTU5-300124/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Product: rtu530					
Affected Version(s): -					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RTU5-300124/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Product: rtu540					
Affected Version(s): -					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RTU5-300124/818
Product: rtu560					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	H-HIT-RTU5-300124/819
Vendor: mediatek					
Product: mt2713					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT27-300124/820

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: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/821
Product: mt2735					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/823
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/825
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT27-300124/827
Product: mt6580					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/829
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/831
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT65-300124/833
Product: mt6731					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895).	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32889		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/835
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/836
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information	https://corp.mediatek.com/product-security-	H-MED-MT67-300124/837

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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	bulletin/January-2024	
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/839
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/840
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/841

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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6737					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/842
Out-of-bounds Write	02-Jan-2024	6.7	In keyInstall, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/844
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT67-300124/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/846
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT67-300124/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/848
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/850
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6753					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/852
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/854
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/855
Product: mt6757					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/856
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/858
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/859
Product: mt6757c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/860
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/862
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/863
Product: mt6757cd					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/864
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/866
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/867
Product: mt6757ch					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/868
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/870
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/871
Product: mt6761					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/872
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/874
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/875
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/877
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT67-300124/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/879
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT67-300124/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/881
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32879		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/883
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/884
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a	https://corp.mediatek.com/product-security-	H-MED-MT67-300124/885

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/886
Out-of-bounds Read	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/888
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. 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/January-2024	H-MED-MT67-300124/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**		
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/890
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT67-300124/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/892
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32876		
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/894
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32872		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/896
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/897
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-300124/898

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/901
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/903
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/905
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/906
Product: mt6768					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/907
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/909
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/910
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/912
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT67-300124/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/914
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT67-300124/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/916
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/918
Product: mt6771					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/920
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/922
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893).	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32874		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/924
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963).	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32890		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/926
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/927
Improper Restriction of Operations	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to	https://corp.mediatek.com/product-security-	H-MED-MT67-300124/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	bulletin/January-2024	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/929
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/931
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/933
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/935
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/937
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/939
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/940
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/941

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/942
Product: mt6783					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/944
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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/January-2024	H-MED-MT67-300124/945

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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/946
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/948
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT67-300124/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/950
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/952
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/954
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/955
Product: mt6785t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/956
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/958
Product: mt6789					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/960
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/962
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/963
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/965
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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/January-2024	H-MED-MT67-300124/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/967
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT67-300124/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32876		
Product: mt6813					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/969
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/971
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/973
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/975
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/977
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/979
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/981
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/983
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/984
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT68-300124/985

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: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/986
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due 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/January-2024	H-MED-MT68-300124/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/988
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/990
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/992
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/993
Product: mt6833p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/994
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/996
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/998
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/999
Product: mt6835					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1000
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1002
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1004
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1006
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1007
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1009
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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/January-2024	H-MED-MT68-300124/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1011
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32876		
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1013
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1015
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1017
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1019
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1021
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1022
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth service, there is a possible out of bounds write due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1024
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1026
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1028
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1030
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1032
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1034
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1036
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893).	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32874		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1038
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892).	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32887		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1040
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1042
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32872		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1044
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1045
Improper Restriction of	02-Jan-2024	6.7	In display drm, there is a possible memory	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1047
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1049
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1051
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1053
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1055
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1057
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32884		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1059
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1060
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1061

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1062
Product: mt6875					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1064
Improper Restriction of Operations within the	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1066
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	bulletin/January-2024	
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1068
Out-of-bounds Write	02-Jan-2024	6.7	In keyInstall, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1070
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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/January-2024	H-MED-MT68-300124/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1072
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32876		
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1074
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1076
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1078
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1080
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1082
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1083
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth service, there is a possible out of bounds write due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1085
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt6877t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1087
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1089
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1091
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Product: mt6878					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1093
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1095
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1097
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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/January-2024	H-MED-MT68-300124/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**		
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1099
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1101
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1103
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1105
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1107
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1109
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1110
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1112
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1114
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1116
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6880					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1118
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1120
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1122
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1124
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1126
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1128
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1130
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1132
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1133
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT68-300124/1134

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: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1135
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due 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/January-2024	H-MED-MT68-300124/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1137
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1139
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1141
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1142
Product: mt6885					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1143
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1145
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1147
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1149
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1150
Out-of-bounds Write	02-Jan-2024	6.7	In battery, 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/January-2024	H-MED-MT68-300124/1151

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: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1152
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1154
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1156
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1157
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1158

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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1159
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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/January-2024	H-MED-MT68-300124/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**		
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1161
Product: mt6886					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1163
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1165
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1167
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1169
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1171
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1172
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1173

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1174
Product: mt6889					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1176
Improper Restriction of Operations within the Bounds of	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1178
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1180
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1182
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1184
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1186
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1187
Product: mt6890					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1188
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1190
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1192
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1193
Use of Insufficient	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	bulletin/January-2024	
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1195
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	bulletin/January-2024	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1197
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1199
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1201
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT68-300124/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1203
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1205
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1207
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1209
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1211
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32872		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1213
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1214
Improper Restriction of	02-Jan-2024	6.7	In display drm, there is a possible memory	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1216
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1218
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1220
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1222
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1224
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT68-300124/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1226
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32884		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1228
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1229
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1230

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1231
Product: mt6895t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1233
Improper Restriction of Operations within the	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1235
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This	https://corp.mediatek.com/product-security-	H-MED-MT68-300124/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1237
Product: mt6896					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1239
Improper Restriction of Operations within the Bounds of	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1241
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1243
Product: mt6897					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1245
Improper Restriction of Operations within the Bounds of	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1247
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT68-300124/1249
Product: mt6980					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1251
Improper Restriction of Operations within the Bounds of	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1253
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1255
Product: mt6980d					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1257
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1259
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1261
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1263
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a 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/January-2024	H-MED-MT69-300124/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1265
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1267
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1268
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1270
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT69-300124/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1272
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**		
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1274
Product: mt6983t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1276
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1278
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1280
Product: mt6983w					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1282
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1284
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1286
Product: mt6983z					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1288
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1290
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1292
Product: mt6985					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1294
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1296
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1298
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32872		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1300
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1301
Improper Restriction of	02-Jan-2024	6.7	In display drm, there is a possible memory	https://corp.mediatek.com/product-security-	H-MED-MT69-300124/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1303
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1305
Product: mt6985t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1307
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1309
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1311
Product: mt6989					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1313
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1315
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1317
Product: mt6990					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1319
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830; Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1321
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT69-300124/1323
Product: mt7612					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**		
Product: mt7613					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1325
Product: mt7615					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**		
Product: mt7622					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1327
Product: mt7626					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**		
Product: mt7629					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT76-300124/1329
Product: mt7915					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT79-300124/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**		
Product: mt7916					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT79-300124/1331
Product: mt7981					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT79-300124/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**		
Product: mt7986					
Affected Version(s): -					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT79-300124/1333
Product: mt8167					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1335
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1337
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1338
Out-of-bounds Read	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1339

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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1340
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**		
Product: mt8167s					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1342
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Product: mt8168					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1344
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32879		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1346
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1347
Improper Restriction of Operations	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to	https://corp.mediatek.com/product-security-	H-MED-MT81-300124/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	bulletin/January-2024	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1349
Out-of-bounds Read	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1351
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. 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/January-2024	H-MED-MT81-300124/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**		
Product: mt8173					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1353
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32884		
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1355
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8185					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1357
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1359
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1360
Product: mt8188					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1361
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1362
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1363

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1364
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1366
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32878		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1368
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1369
Product: mt8192					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1370
Product: mt8195					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1371
Improper Restriction of	02-Jan-2024	6.7	In netdagent, there is a possible information	https://corp.mediatek.com/product-security-	H-MED-MT81-300124/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	bulletin/January-2024	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1373
Product: mt8195z					
Affected Version(s): -					
Improper Restriction of Operations within the	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT81-300124/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Product: mt8321					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1375
Out-of-bounds Write	02-Jan-2024	6.7	In keyInstall, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	H-MED-MT83-300124/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1377
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of 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/January-2024	H-MED-MT83-300124/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1379
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32883		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1381
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1383
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1384
Out-of-bounds Read	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-300124/1385

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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	bulletin/January-2024	
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1386
Product: mt8362a					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT83-300124/1387

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: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1388
Product: mt8365					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a 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/January-2024	H-MED-MT83-300124/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1390
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1392
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1394
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1396
Product: mt8390					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1397
Product: mt8395					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1398
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT83-300124/1399
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of	https://corp.mediatek.com/product-security-	H-MED-MT86-300124/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1401
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, 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/January-2024	H-MED-MT86-300124/1402

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: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1403
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT86-300124/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1405
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1407
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32883		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1409
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1411
Product: mt8673					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1413
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1415
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1416
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1417

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1418
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1420
Out-of-bounds Write	02-Jan-2024	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/January-2024	H-MED-MT86-300124/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1422
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT86-300124/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Product: mt8676					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1424
Product: mt8696					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT86-300124/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Product: mt8755					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1426
Product: mt8765					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1428
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a 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/January-2024	H-MED-MT87-300124/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1430
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1432
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1433
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1434

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1435
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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/January-2024	H-MED-MT87-300124/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1437
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**		
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1439
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1441
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1443
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1444
Improper Restriction of Operations within the Bounds of	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1446
Out-of-bounds Read	02-Jan-2024	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/January-2024	H-MED-MT87-300124/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1448
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1450
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1452
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1454
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1455
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1456

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1457
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1459
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1461
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1463
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1464
Product: mt8771					
Affected Version(s): -					
Improper Restriction	02-Jan-2024	6.7	In netdagent, there is a possible	https://corp.mediatek.com/pro	H-MED-MT87-300124/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	duct-security-bulletin/January-2024	
Product: mt8775					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1466
Product: mt8781					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1467
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1469
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1470
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1471

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1472
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1474
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1476
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1478
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1479
Product: mt8786					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1480
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1482
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1483
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1484

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1485
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1487
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32876		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1489
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1490
Integer Overflow	02-Jan-2024	4.4	In battery, there is a possible	https://corp.mediatek.com/pro	H-MED-MT87-300124/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	duct-security-bulletin/January-2024	
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1493
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1494
Out-of-bounds Write	02-Jan-2024	6.7	In battery, 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/January-2024	H-MED-MT87-300124/1495

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: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1496
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1498
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1500
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1501
Out-of-bounds Read	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-300124/1502

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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	bulletin/January-2024	
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1503
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1505
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a 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/January-2024	H-MED-MT87-300124/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1507
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32882		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1509
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1510
Improper Restriction of	02-Jan-2024	6.7	In display drm, there is a possible memory	https://corp.mediatek.com/product-security-	H-MED-MT87-300124/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	bulletin/January-2024	
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1512
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1513

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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1514
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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/January-2024	H-MED-MT87-300124/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**		
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1516
Product: mt8791					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1518
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1520
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1522
Product: mt8791t					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1524
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1526
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1527
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1528

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1529
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1531
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1533
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1535
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1536
Product: mt8792					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1537
Product: mt8795t					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8796					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1539
Product: mt8797					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1541
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32872		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1543
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1544
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-300124/1545

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1546
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1548
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612;	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1550
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1552
Product: mt8798					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1554
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1556
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1557
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1558

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: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1559
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1561
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08304217.	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32875		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1563
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1565
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	H-MED-MT87-300124/1566
Product: mt8871					
Affected Version(s): -					
Improper Restriction	02-Jan-2024	6.7	In netdagent, there is a possible	https://corp.mediatek.com/pro	H-MED-MT88-300124/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	duct-security-bulletin/January-2024	
Vendor: Qualcomm					
Product: 315_5g_iot_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1568
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1569
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1571
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1572
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1573
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-315_-300124/1574
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-315_-300124/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-315_-300124/1576
Product: 9205_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-9205-300124/1577
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-9205-300124/1578
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-9205-300124/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 9206_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9206-300124/1580
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9206-300124/1581
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9206-300124/1582
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9206-300124/1583
Product: 9207_lte_modem					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9207-300124/1584
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-9207-300124/1585
Product: apq8017					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1586
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1587
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1589
Product: apq8037					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1590
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1591
Product: apq8064au					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1592
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-APQ8-300124/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1594
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1595
Product: apq8076					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1596
Product: apq8084					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-APQ8-300124/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Product: apq8092					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1598
Product: apq8094					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-APQ8-300124/1599
Product: aqt1000					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets an IPv6 address. **CVE ID : CVE-2023-28583**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1601
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1602
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1603
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1604
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1606
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1607
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1608
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1609
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-AQT1-300124/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AQT1-300124/1611
Product: ar8031					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1612
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1613
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1615
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1616
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1617
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1618
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-AR80-300124/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: ar8035					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1620
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1621
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1622
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1624
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1625
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1626
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1627
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-AR80-300124/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1629
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1630
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1632
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1633
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1634
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1635
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1636
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-AR80-300124/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1638
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR80-300124/1639
Product: ar9380					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR93-300124/1640
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR93-300124/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR93-300124/1642
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-AR93-300124/1643
Product: c-v2x_9150					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-C-V2-300124/1644
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-C-V2-300124/1645
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-C-V2-300124/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-C-V2-300124/1647
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-C-V2-300124/1648
Product: csr8811					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSR8-300124/1649
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-CSR8-300124/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSR8-300124/1651
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSR8-300124/1652
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSR8-300124/1653
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSR8-300124/1654
Product: csra6620					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1655
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1656
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1657
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1658
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1659
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager	https://www.qualcomm.com/company/produc	H-QUA-CSRA-300124/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1661
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1662
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1664
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1665
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1666
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1667
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1669
Product: csra6640					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1670
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1671
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1672
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	H-QUA-CSRA-300124/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1674
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1675
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1676
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1678
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1679
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1680
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1682
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1683
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRA-300124/1684
Product: csrb31024					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1685
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-CSRB-300124/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1687
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1688
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1689
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1690
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-CSRB-300124/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1692
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-CSRB-300124/1693
Product: fastconnect_6200					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1694
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1696
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1697
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1698
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1699
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1701
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1702
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1703
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1705
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1706
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1707
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1708
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-FAST-300124/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-FAST-300124/1710
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-FAST-300124/1711
NULL Pointer Dereferenc e	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-FAST-300124/1712
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-FAST-300124/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fastconnect_6700					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1714
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1715
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1716
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1717
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1719
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1720
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1721
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1723
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1724
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1725
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-FAST-300124/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1727
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1728
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1729
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1730
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-FAST-300124/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: fastconnect_6800					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1732
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1733
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1734
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1735
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	H-QUA-FAST-300124/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1737
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1738
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1740
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1741
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1742
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1743
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1745
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1746
Product: fastconnect_6900					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1747
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1748
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-FAST-300124/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1751
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1752
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1753
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	H-QUA-FAST-300124/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1755
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1756
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1758
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1759
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1760
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1761
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1763
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1764
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1765
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1766
Product: fastconnect_7800					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1767
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1768
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1770
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1772
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1773
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1774
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1776
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1777
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1778
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1779
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1781
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1782
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1783
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FAST-300124/1784
Product: flight_rb5_5g_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1785
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1787
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1788
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1790
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1791
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1792
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-FLIG-300124/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1794
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1795
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1796
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1797
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/produc	H-QUA-FLIG-300124/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FLIG-300124/1799
Product: fsm10056					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FSM1-300124/1800
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-FSM1-300124/1801
Product: home_hub_100_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-HOME-300124/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-HOME-300124/1803
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-HOME-300124/1804
Product: immersive_home_214_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1805
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1806
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	H-QUA-IMME-300124/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1808
Product: immersive_home_216_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1809
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1810
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1812
Product: immersive_home_316_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1813
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1814
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1815
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IMME-300124/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: immersive_home_318_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1817
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1818
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1819
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: immersive_home_3210_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1821
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1822
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1823
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1824
Product: immersive_home_326_platform					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	H-QUA-IMME-300124/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1826
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1827
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IMME-300124/1828
Product: ipq4018					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1830
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1831
Product: ipq4019					
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1832
Product: ipq4028					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1833
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/produc	H-QUA-IPQ4-300124/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1835
Product: ipq4029					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1836
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1837
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ4-300124/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: ipq5010					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1839
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1840
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1841
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1842
Product: ipq5028					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1843
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1844
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1845
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1846
Product: ipq5332					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ5-300124/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ5-300124/1848
Product: ipq6000					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1849
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1850
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1852
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1853
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1854
Product: ipq6005					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1855
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ6-300124/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032	ns/january-2024-bulletin	
Product: ipq6010					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1857
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1858
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1859
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1860
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1862
Product: ipq6018					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1863
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1864
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1865
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-IPQ6-300124/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1867
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1868
Product: ipq6028					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1869
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1871
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1872
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1873
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ6-300124/1874
Product: ipq8064					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-300124/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1876
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1877
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1878
Product: ipq8065					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1879
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-300124/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1881
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1882
Product: ipq8068					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1883
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1885
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1886
Product: ipq8069					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1887
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1888
Product: ipq8070					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1889
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1890
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1891
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1892
Product: ipq8070a					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-300124/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1894
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1895
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1896
Product: ipq8071a					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1897
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-300124/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1899
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1900
Product: ipq8072a					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1901
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-IPQ8-300124/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1903
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1904
Product: ipq8074					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1905
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1906
Product: ipq8074a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1907
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1908
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1909
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1910
Product: ipq8076					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-300124/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1912
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1913
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1914
Product: ipq8076a					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1915
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-300124/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1917
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1918
Product: ipq8078					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1919
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1921
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1922
Product: ipq8078a					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1923
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1924
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-300124/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1926
Product: ipq8173					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1927
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1928
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1929
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-300124/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: ipq8174					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1931
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1932
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1933
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ8-300124/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: ipq9008					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1935
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1936
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1937
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1938
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ9-300124/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: ipq9554					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1940
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1941
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1942
Product: ipq9570					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ9-300124/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1944
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1945
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1946
Product: ipq9574					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1947
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/c	H-QUA-IPQ9-300124/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1949
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1950
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-IPQ9-300124/1951
Product: mdm8207					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM8-300124/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM8-300124/1953
Product: mdm9225					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1954
Product: mdm9225m					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1955
Product: mdm9230					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1956
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-300124/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Product: mdm9235m					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1958
Product: mdm9250					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1959
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1960
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1962
Product: mdm9330					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1963
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1964
Product: mdm9625					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1965
Product: mdm9625m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1966
Product: mdm9628					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1967
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1968
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1969
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-300124/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: mdm9630					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1971
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1972
Product: mdm9635m					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1973
Product: mdm9640					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-300124/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1975
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1976
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1977
Product: mdm9645					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: mdm9650					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1979
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1980
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1981
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1982
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	H-QUA-MDM9-300124/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MDM9-300124/1984
Product: msm8108					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1985
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1986
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Product: msm8209					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1988
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1989
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1990
Product: msm8608					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1991
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/produc	H-QUA-MSM8-300124/1992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1993
Product: msm8909w					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1994
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1995
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1997
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1998
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/1999
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-MSM8-300124/2000
Product: pm8937					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-PM89-300124/2001
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-PM89-300124/2002
Product: pmp8074					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-PMP8-300124/2003
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-PMP8-300124/2004
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-PMP8-300124/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qam8255p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2007
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2008
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2009
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager	https://www.qualcomm.com/company/produc	H-QUA-QAM8-300124/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2011
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2012
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2014
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2015
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2016
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2017
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2019
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2020
Product: qam8295p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2021
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2022
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-QAM8-300124/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2024
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2025
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2026
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2028
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2029
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2030
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	H-QUA-QAM8-300124/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2032
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2033
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2034
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2036
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2037
Product: qam8650p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2039
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QAM8-300124/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2041
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2042
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2043
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2045
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2046
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2047
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2048
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	H-QUA-QAM8-300124/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2050
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2051
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2052
Product: qam8775p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QAM8-300124/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2054
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2055
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2056
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2057
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-QAM8-300124/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2059
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2060
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2062
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2063
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2064
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2065
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QAM8-300124/2067
Product: qca0000					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA0-300124/2068
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA0-300124/2069
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA0-300124/2070
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA0-300124/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qca1023					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2072
Product: qca1062					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2073
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2074
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA1-300124/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qca1064					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2076
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2077
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA1-300124/2078
Product: qca1990					
Affected Version(s): -					
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCA1-300124/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qca2062					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2080
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2081
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2082
Product: qca2064					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	H-QUA-QCA2-300124/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2084
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2085
Product: qca2065					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2086
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2088
Product: qca2066					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2089
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2090
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA2-300124/2091
Product: qca4004					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2092
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2093
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2094
Product: qca4024					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2095
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2097
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2098
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2099
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA4-300124/2100
Product: qca4531					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA4-300124/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qca6174					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2102
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2103
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2104
Product: qca6174a					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2106
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2107
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2109
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2111
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2112
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2113
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2115
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2116
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2117
Product: qca6175a					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: qca6234					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2119
Product: qca6310					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2120
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2121
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2123
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2124
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2125
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2126
Product: qca6320					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2128
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2129
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2130
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2131
Product: qca6335					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2132
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2133
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2134
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2135
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2136
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2138
Product: qca6391					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2139
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2140
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2143
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2144
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2145
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	H-QUA-QCA6-300124/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2147
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2148
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2150
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2151
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2152
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2153
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2155
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2156
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2157
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2158
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in Automotive while	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	t-security/bulletins/january-2024-bulletin	
Product: qca6420					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2160
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2161
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2162
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2164
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2165
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2166
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2168
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2169
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2170
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2171
Product: qca6421					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2173
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2174
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2175
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2177
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2178
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2179
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2180
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2182
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2183
Product: qca6426					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2184
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2185
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2187
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2188
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2189
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2191
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2192
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2193
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2195
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2196
Product: qca6428					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2197
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2198
Product: qca6430					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2199
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2200
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2201
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2202
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2204
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2205
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2206
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2207
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2209
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2210
Product: qca6431					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2211
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2213
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2214
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2215
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2217
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2218
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2219
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2220
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036	ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2222
Product: qca6436					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2223
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2224
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2225
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2227
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2228
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2229
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2231
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2232
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2233
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2234
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	ompany/product-security/bulletins/january-2024-bulletin	
Product: qca6438					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2236
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2237
Product: qca6554a					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2239
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2240
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2241
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2242
Product: qca6564					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2244
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2245
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2246
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2247
Product: qca6564a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2248
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2249
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2250
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2251
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2253
Product: qca6564au					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2254
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2255
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2256
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2258
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2259
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2260
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2261
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2263
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2264
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2265
Product: qca6574					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2267
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2268
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2269
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2270
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33108		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2272
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2273
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2274
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2276
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2277
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2278
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2280
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2281
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2282
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2283
Product: qca6574a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2284
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2285
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2286
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2288
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2290
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2291
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2292
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2294
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2295
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2297
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2298
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2299
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2300
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2302
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2303
Product: qca6574au					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2304
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2305
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	H-QUA-QCA6-300124/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2307
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2309
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2310
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2312
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2313
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2314
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2316
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2317
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2318
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2320
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2321
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2322
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2323
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the	https://www.qualcomm.com/company/product-	H-QUA-QCA6-300124/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	security/bulletins/january-2024-bulletin	
Product: qca6584					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2325
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2326
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2327
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2329
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2330
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2331
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2332
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	H-QUA-QCA6-300124/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2334
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2335
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2336
Product: qca6595					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2338
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2340
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2341
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33108		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2343
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2344
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2345
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2347
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2348
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2349
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2351
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2352
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2353
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2354
Product: qca6595au					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2355
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2356
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2357
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2358
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2359
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2361
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2362
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2363
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-QCA6-300124/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2365
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2366
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2368
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2369
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2370
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2371
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2373
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2374
Product: qca6678aq					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2375
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2376
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: qca6696					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2378
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2379
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2380
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2383
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2384
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2385
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-300124/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2387
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2388
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2390
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2391
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2392
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2393
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2395
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2396
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2397
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2398
Product: qca6698aq					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2399
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2400
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2402
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2403
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2405
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2406
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2408
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2409
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2410
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2412
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2413
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2414
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2415
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2417
Product: qca6797aq					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2418
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2419
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2420
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a	https://www.qualcomm.com/company/product-	H-QUA-QCA6-300124/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2422
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2423
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2424
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-QCA6-300124/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2426
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2427
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2428
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2430
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2431
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA6-300124/2432
Product: qca7500					
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA7-300124/2433
Product: qca8072					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2434
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2435
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2436
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2437
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca8075					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2439
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2440
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2441
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2442
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2444
Product: qca8081					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2445
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2446
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2447
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-QCA8-300124/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2449
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2450
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2451
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2452
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-QCA8-300124/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2454
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2455
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2457
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2458
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2459
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2460
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2461
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCA8-300124/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2463
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2464
Product: qca8082					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2465
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-300124/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2467
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2468
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2469
Product: qca8084					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2470
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/c	H-QUA-QCA8-300124/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2472
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2473
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2474
Product: qca8085					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032		
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2476
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2477
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2478
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2479
Product: qca8337					
Affected Version(s): -					
Buffer Copy without Checking	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP	https://www.qualcomm.com/company/product-	H-QUA-QCA8-300124/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			body, during a VOLTE call. **CVE ID : CVE-2023-33025**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2481
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2482
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2483
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2484
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-300124/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2486
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2487
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2488
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	H-QUA-QCA8-300124/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2490
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2491
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2492
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-300124/2493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2494
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2495
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2496
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2497
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-300124/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			support makes a PSCI call. **CVE ID : CVE-2023-33036**	ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2499
Product: qca8386					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2500
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2501
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2503
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA8-300124/2504
Product: qca9367					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2505
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2506
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2508
Product: qca9377					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2509
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2510
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2513
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2514
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2515
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	H-QUA-QCA9-300124/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2517
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2518
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2519
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2521
Product: qca9379					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2522
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2523
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2524
Product: qca9880					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2525
Product: qca9886					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2526
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2527
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2528
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: qca9888					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2530
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2531
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2532
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2533
Product: qca9889					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2534
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2535
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2536
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2537
Product: qca9898					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA9-300124/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2539
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2540
Product: qca9980					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2541
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2543
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2544
Product: qca9984					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2545
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2546
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2548
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2549
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2550
Product: qca9985					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2551
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA9-300124/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2553
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2554
Product: qca9986					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2555
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2556
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCA9-300124/2557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qca9990					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2558
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2559
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2560
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qca9992					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2562
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2563
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2564
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2565
Product: qca9994					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2566
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2567
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2568
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCA9-300124/2569
Product: qcc2073					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCC2-300124/2570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC2-300124/2571
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC2-300124/2572
Product: qcc2076					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC2-300124/2573
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC2-300124/2574
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-QCC2-300124/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qcc710					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2576
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2577
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2579
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2580
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2581
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCC7-300124/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcf8001					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCF8-300124/2583
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCF8-300124/2584
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCF8-300124/2585
Product: qcm2290					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2586
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/produc	H-QUA-QCM2-300124/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2588
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2589
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2590
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM2-300124/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2592
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2593
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2594
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM2-300124/2595
Product: qcm4290					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2596
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2597
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2598
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2599
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2601
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2602
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2603
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2604
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM4-300124/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qcm4325					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2606
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2608
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2610
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2611
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2612
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2614
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2615
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2616
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2617
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2619
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2620
Product: qcm4490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2621
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2623
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2624
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2625
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2626
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2627
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-QCM4-300124/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2629
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2630
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM4-300124/2631
Product: qcm6125					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM6-300124/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2633
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2634
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2635
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2636
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	H-QUA-QCM6-300124/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2638
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2639
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2640
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2641
Product: qcm6490					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2642
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2643
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2645
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2647
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2648
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2649
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2651
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2652
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2653
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2654
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM6-300124/2656
Product: qcm8550					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2657
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2658
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2660
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2661
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2662
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM8-300124/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2664
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2665
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCM8-300124/2666
Product: qcn5021					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2668
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2669
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2670
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2671
Product: qcn5022					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN5-300124/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2673
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2674
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2675
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2676
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn5024					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2678
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2679
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2680
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2681
Product: qcn5052					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2682
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2683
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2684
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2685
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2686
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCN5-300124/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qcn5054					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2688
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2689
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2690
Product: qcn5121					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/produc	H-QUA-QCN5-300124/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2692
Product: qcn5122					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2693
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2694
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2695
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN5-300124/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2697
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2698
Product: qcn5124					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2699
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2701
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2702
Product: qcn5152					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2703
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2704
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN5-300124/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2706
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2707
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2708
Product: qcn5154					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2709
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-QCN5-300124/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN5-300124/2711
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN5-300124/2712
Product: qcn5164					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN5-300124/2713
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN5-300124/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2715
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN5-300124/2716
Product: qcn6023					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2717
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2718
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN6-300124/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2720
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2721
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2722
Product: qcn6024					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2724
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2725
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2726
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2728
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-QCN6-300124/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2730
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2731
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2732
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2733
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	H-QUA-QCN6-300124/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2735
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2736
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2737
Product: qcn6100					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2739
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2740
Product: qcn6102					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2741
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2742
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN6-300124/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qcn6112					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2744
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2745
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2746
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn6122					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2748
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2749
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2750
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2751
Product: qcn6132					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2752
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2753
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2754
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2755
Product: qcn6224					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN6-300124/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2757
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2758
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2759
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-QCN6-300124/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN6-300124/2761
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN6-300124/2762
Product: qcn6274					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODU LE command. **CVE ID : CVE-2023-33117**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-QCN6-300124/2763
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.q ualcomm.com/c ompany/produc t-	H-QUA-QCN6-300124/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2765
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2766
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2767
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN6-300124/2768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN6-300124/2769
Product: qcn7605					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2770
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2771
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn7606					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2773
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2774
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2775
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN7-300124/2776
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing GATT service data when the total amount of memory that is required by	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN7-300124/2777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the multiple services is greater than the actual size of the services buffer. **CVE ID : CVE-2023-43512**	ns/january-2024-bulletin	
Product: qcn9000					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2778
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2779
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2780
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2782
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2783
Product: qcn9001					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2784
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2785
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN9-300124/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qcn9002					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2787
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2788
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2789
Product: qcn9003					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN9-300124/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2791
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2792
Product: qcn9011					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2793
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2794
Buffer Copy without Checking	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/product-	H-QUA-QCN9-300124/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2796
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2797
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2798
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN9-300124/2799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2800
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2801
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2802
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2804
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2805
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2806
Product: qcn9012					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2807
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-QCN9-300124/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2809
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2810
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2811
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2813
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2814
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2815
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCN9-300124/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2817
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2818
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2819
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2820
Product: qcn9013					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/c	H-QUA-QCN9-300124/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2822
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2823
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2824
Product: qcn9022					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2826
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2827
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2828
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2829
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9024					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2831
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2832
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2833
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2834
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2836
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2837
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2838
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2839
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2841
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2842
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2843
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2844
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33037		
Product: qcn9070					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2846
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2847
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2848
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2849
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2851
Product: qcn9072					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2852
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2853
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2854
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-QCN9-300124/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2856
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2857
Product: qcn9074					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2858
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2860
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2861
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2862
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2863
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2864
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-QCN9-300124/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: qcn9100					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2866
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2867
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2868
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: qcn9274					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2870
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2871
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2872
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCN9-300124/2873
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-QCN9-300124/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qcs2290					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2875
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2876
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2877
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2879
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2880
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2881
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2882
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-QCS2-300124/2883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS2-300124/2884
Product: qcs410					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2885
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2886
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2888
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2889
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2890
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2891
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECU	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2893
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2894
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2895
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/c	H-QUA-QCS4-300124/2896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2897
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2898
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2899
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2900
Product: qcs4290					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2901
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2902
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2903
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2904
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2906
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2907
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2908
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2909
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS4-300124/2910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qcs4490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2911
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2912
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2913
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2915
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2916
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2917
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2918
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2919
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-QCS4-300124/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS4-300124/2921
Product: qcs610					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2922
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2923
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-300124/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2925
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2926
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2927
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2928
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-300124/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2930
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2931
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2933
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2934
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2935
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2936
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcs6125					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2938
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2939
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2940
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2941
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-300124/2942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2943
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2944
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2945
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2946
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-QCS6-300124/2947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qcs6490					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2948
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2949
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2952
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2953
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2954
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2956
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2957
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2958
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2960
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2961
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2962
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS6-300124/2963
Product: qcs7230					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS7-300124/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2965
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2966
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2967
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS7-300124/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2969
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2970
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2971
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2973
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS7-300124/2974
Product: qcs8155					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2975
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2976
Product: qcs8250					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2977
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2978
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2979
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2980
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2982
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2983
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2984
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS8-300124/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2986
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2987
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2988
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2989
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-QCS8-300124/2990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qcs8550					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2991
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2992
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2993
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2995
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2996
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2997
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/2999
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3000
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3001
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3002
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3004
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3005
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3006
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QCS8-300124/3007
Product: qdu1000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3008
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3009
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3010
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3011
Product: qdu1010					
Affected Version(s): -					
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-QDU1-300124/3012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3013
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3014
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3015
Product: qdu1110					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QDU1-300124/3016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3017
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3018
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3019
Product: qdu1210					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3021
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3022
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDU1-300124/3023
Product: qdx1010					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3024
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager	https://www.qualcomm.com/company/produc	H-QUA-QDX1-300124/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3026
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3027
Product: qdx1011					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3028
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QDX1-300124/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3030
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QDX1-300124/3031
Product: qet4101					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QET4-300124/3032
Product: qfw7114					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3034
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3035
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3036
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-QFW7-300124/3037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3038
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3039
Product: qfw7124					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3040
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QFW7-300124/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3042
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3043
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3044
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QFW7-300124/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QFW7-300124/3046
Product: qrb5165m					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3047
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3049
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK	https://www.qualcomm.com/company/produc	H-QUA-QRB5-300124/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3051
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3052
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3053
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-QRB5-300124/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3055
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3056
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3057
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QRB5-300124/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3059
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3060
Product: qrb5165n					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3061
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3062
Buffer Copy without Checking Size of	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QRB5-300124/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3064
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3065
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3066
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3068
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3069
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3070
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	H-QUA-QRB5-300124/3071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3072
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3073
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3074
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRB5-300124/3075
Product: qru1032					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3076
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3077
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3078
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3079
Product: qru1052					
Affected Version(s): -					
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-QRU1-300124/3080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3081
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3082
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3083
Product: qru1062					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QRU1-300124/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3085
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3086
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QRU1-300124/3087
Product: qsm8250					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3089
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3090
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3091
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3092
Product: qsm8350					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QSM8-300124/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3094
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3095
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3096
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSM8-300124/3097
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QSM8-300124/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: qsw8573					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QSW8-300124/3099
Product: qts110					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QTS1-300124/3100
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QTS1-300124/3101
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QTS1-300124/3102
Product: qualcomm_205_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3103
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3104
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3105
Product: qualcomm_215_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3106
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3108
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3109
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3110
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Product: qualcomm_video_collaboration_vc1_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3112
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3113
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3114
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3116
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3117
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3118
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QUAL-300124/3119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3120
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3121
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3122
Product: qualcomm_video_collaboration_vc3_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3124
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3125
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3126
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3128
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3129
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3130
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3132
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3133
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3134
Product: qualcomm_video_collaboration_vc5_platform					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3135
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a	https://www.qualcomm.com/company/product-	H-QUA-QUAL-300124/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3137
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3138
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3140
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3141
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3142
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3143
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-QUAL-300124/3144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3145
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-QUAL-300124/3146
Product: robotics_rb3_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3147
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3149
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3150
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3151
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3152
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-ROBO-300124/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			support makes a PSCI call. **CVE ID : CVE-2023-33036**	ns/january-2024-bulletin	
Product: robotics_rb5_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3154
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3155
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3156
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3157
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	H-QUA-ROBO-300124/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3159
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3160
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3162
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3163
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3164
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3165
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	H-QUA-ROBO-300124/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3167
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-ROBO-300124/3168
Product: sa4150p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3169
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3171
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3172
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3173
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3174
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3176
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3177
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3178
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	H-QUA-SA41-300124/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3180
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3181
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3182
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa4155p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3184
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3185
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3187
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3189
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3190
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3191
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3193
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3194
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3195
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA41-300124/3197
Product: sa6145p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3198
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3199
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3200
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SA61-300124/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3203
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3204
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3205
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	H-QUA-SA61-300124/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3207
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3208
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3210
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3211
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3212
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3213
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3215
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3216
Product: sa6150p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3217
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3219
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3220
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3222
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3224
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3225
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3226
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3228
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3229
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3230
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3231
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA61-300124/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3233
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3234
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3235
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3237
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3238
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3239
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3240
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3242
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3243
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3244
Product: sa6155p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3246
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3247
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3248
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3250
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-SA61-300124/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3252
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3253
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3254
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-SA61-300124/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3256
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3257
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3259
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3260
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3261
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3262
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3264
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA61-300124/3265
Product: sa8145p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3266
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3267
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	H-QUA-SA81-300124/3268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3269
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3271
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3272
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3274
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3275
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3277
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3278
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3279
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3280
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3282
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3283
Product: sa8150p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3284
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3286
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3287
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3288
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3289
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3291
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3292
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3293
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3295
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3296
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3297
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3298
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3300
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3301
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3302
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3304
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3305
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3306
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3307
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3309
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3310
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3311
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3312
Product: sa8155p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer	https://www.qualcomm.com/company/produc	H-QUA-SA81-300124/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3314
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3315
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3316
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3317
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-SA81-300124/3318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3319
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3320
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3321
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3323
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3324
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3325
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	H-QUA-SA81-300124/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3327
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3328
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3329
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3330
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-SA81-300124/3331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3332
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3333
Product: sa8195p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3334
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/product-	H-QUA-SA81-300124/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3336
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3337
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3338
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3339
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3341
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3342
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3343
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-300124/3344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3345
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3346
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3347
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/c	H-QUA-SA81-300124/3348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3349
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3350
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3351
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA81-300124/3352
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in	https://www.qualcomm.com/c	H-QUA-SA81-300124/3353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	ompany/product-security/bulletins/january-2024-bulletin	
Product: sa8255p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3354
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3355
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3356
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33108		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3358
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3359
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3360
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA82-300124/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3362
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3363
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3364
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3365
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-SA82-300124/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3367
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3368
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3369
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3371
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3372
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3373
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3374
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLO	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA82-300124/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3376
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3377
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3379
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3380
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3381
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3382
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3384
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA82-300124/3385
Product: sa8540p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA85-300124/3386
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA85-300124/3387
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in	https://www.qualcomm.com/c	H-QUA-SA85-300124/3388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	ompany/product-security/bulletins/january-2024-bulletin	
Product: sa9000p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA90-300124/3389
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA90-300124/3390
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SA90-300124/3391
Product: sc8180x\+sdx55					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SC81-300124/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SC81-300124/3393
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SC81-300124/3394
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SC81-300124/3395
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SC81-300124/3396
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SC81-300124/3397
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a	https://www.qualcomm.com/c	H-QUA-SC81-300124/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ompany/produc t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SC81-300124/3399
Product: sd460					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SD46-300124/3400
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SD46-300124/3401
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SD46-300124/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD46-300124/3403
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD46-300124/3404
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD46-300124/3405
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD46-300124/3406
Product: sd626					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	H-QUA-SD62-300124/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD62-300124/3408
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD62-300124/3409
Product: sd660					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3410
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3411
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD66-300124/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3413
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3414
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3416
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3417
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3418
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3419
Product: sd662					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/produc	H-QUA-SD66-300124/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3421
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3422
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3423
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3424
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD66-300124/3426
Product: sd670					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3427
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3428
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3429
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	H-QUA-SD67-300124/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3431
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3432
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3433
Product: sd675					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3435
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3436
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3437
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3438
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3440
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3441
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3442
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD67-300124/3443
Product: sd730					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD73-300124/3444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3445
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3446
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3447
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3448
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	H-QUA-SD73-300124/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3450
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3451
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3452
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD73-300124/3453
Product: sd820					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD82-300124/3454
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD82-300124/3455
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD82-300124/3456
Product: sd821					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD82-300124/3457
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD82-300124/3458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: sd835					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD83-300124/3459
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD83-300124/3460
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD83-300124/3461
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD83-300124/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD83-300124/3463
Product: sd855					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3464
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3465
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3467
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3468
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3469
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3470
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-SD85-300124/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3472
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3473
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3474
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD85-300124/3475
Product: sd865_5g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3476
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3477
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3478
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3479
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3481
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3482
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3483
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD86-300124/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3485
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3486
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3487
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD86-300124/3488
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD86-300124/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: sd888					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3490
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3491
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3493
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	H-QUA-SD88-300124/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3495
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3496
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3497
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	H-QUA-SD88-300124/3498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3499
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3500
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3501
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD88-300124/3502
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD88-300124/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: sdm429w					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDM4-300124/3504
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDM4-300124/3505
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDM4-300124/3506
Product: sdx20m					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SDX2-300124/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX2-300124/3508
Product: sdx55					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3509
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3510
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3513
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3514
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3516
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3517
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3518
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3519
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3521
Product: sdx57m					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3522
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3523
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3524
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX5-300124/3526
Product: sdx65m					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX6-300124/3527
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX6-300124/3528
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX6-300124/3529
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SDX6-300124/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: sd_455					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_4-300124/3531
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_4-300124/3532
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_4-300124/3533
Product: sd_675					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3535
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3536
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3537
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3538
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3540
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3541
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3542
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_6-300124/3543
Product: sd_8cx					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_8-300124/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3545
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3546
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3547
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3548
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_8-300124/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036	ns/january-2024-bulletin	
Product: sd_8_gen1_5g					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3550
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3551
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3552
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3553
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_8-300124/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3555
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3556
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SD_8-300124/3557
Product: sg4150p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3559
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3560
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3561
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3562
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SG41-300124/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3564
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3565
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3566
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3568
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3569
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG41-300124/3570
Product: sg8275p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3571
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-SG82-300124/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3573
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3574
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3575
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-SG82-300124/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3577
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3578
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SG82-300124/3579
Product: sm4125					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3580
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3581
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3582
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3583
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	H-QUA-SM41-300124/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3585
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3586
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3587
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM41-300124/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: sm4450					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM44-300124/3589
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM44-300124/3590
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM44-300124/3591
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM44-300124/3592
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/product-	H-QUA-SM44-300124/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM44-300124/3594
Product: sm6250					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3595
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3596
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3597
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	H-QUA-SM62-300124/3598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3599
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3600
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3601
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM62-300124/3602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3603
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3604
Product: sm6250p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3605
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3607
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3608
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3609
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3610
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM62-300124/3611
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-SM62-300124/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: sm7250p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3613
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3614
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3615
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3617
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3618
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3619
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM72-300124/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3621
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3622
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3623
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3624
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-SM72-300124/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM72-300124/3626
Product: sm7315					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3627
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3628
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3629
Buffer Copy	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-SM73-300124/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			wearables while processing data from AON. **CVE ID : CVE-2023-33085**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3631
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3632
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3633
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM73-300124/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3635
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3636
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3637
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3638
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives	https://www.qualcomm.com/company/produc	H-QUA-SM73-300124/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3640
Product: sm7325p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3641
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3642
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3644
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3645
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3646
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3647
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	H-QUA-SM73-300124/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3649
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3650
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3651
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3653
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM73-300124/3654
Product: sm8550p					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3655
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3656
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-SM85-300124/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3658
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3659
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3661
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3662
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3663
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SM85-300124/3664
Product: smart_audio_200_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SMAR-300124/3665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3666
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3667
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3668
Product: smart_audio_400_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3670
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3671
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3672
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3673
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3675
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3676
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3677
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SMAR-300124/3678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3679
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3680
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3681
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3682
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SMAR-300124/3683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: smart_display_200_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3684
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3685
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SMAR-300124/3686
Product: snapdragon_1100_wearable_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3688
Product: snapdragon_1200_wearable_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3689
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3690
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3691
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Product: snapdragon_208_processor					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3693
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3694
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3695
Product: snapdragon_210_processor					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3697
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3698
Product: snapdragon_212_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3699
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3700
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Product: snapdragon_425_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3702
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3703
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3704
Product: snapdragon_427_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3705
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3706
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3707
Product: snapdragon_429_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3709
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3710
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3711
Product: snapdragon_430_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3713
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3714
Product: snapdragon_435_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3715
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3717
Product: snapdragon_439_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3718
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3719
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_450_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3721
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3722
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_460_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3724
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3725
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3726
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3728
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3729
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3730
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3732
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3733
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3734
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_480\+_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3736
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3737
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3738
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3740
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3741
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3742
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3744
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3745
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3746
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3747
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3749
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3750
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3751
Product: snapdragon_480_5g_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3752
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3753
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3754
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3755
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3757
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3758
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3759
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3761
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3762
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3763
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3764
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3766
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3767
Product: snapdragon_4_gen_1_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3769
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3771
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3772
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3774
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3775
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3776
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3778
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3779
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3780
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3781
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: snapdragon_4_gen_2_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3783
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3784
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3785
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3786
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: snapdragon_625_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3788
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3789
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3790
Product: snapdragon_626_mobile_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3791
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3792
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3793
Product: snapdragon_630_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3795
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3796
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3797
Product: snapdragon_632_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3798
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3799
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3800
Product: snapdragon_636_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3802
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3803
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3804
Product: snapdragon_660_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3806
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3807
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3808
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3810
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3811
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3812
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3814
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3815
Product: snapdragon_662_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3816
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3818
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3819
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3820
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3822
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3823
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3824
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3826
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3827
Product: snapdragon_665_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3828
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3830
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3831
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3832
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3834
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3835
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3836
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3837
Concurrent Execution using Shared Resource with Improper	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_670_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3839
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3840
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3841
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3843
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3844
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3846
Product: snapdragon_675_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3847
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3848
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3849
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3851
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3852
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3853
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3854
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3856
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3857
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_678_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3859
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3860
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3861
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3862
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3864
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3865
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3866
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3867
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3869
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3870
Product: snapdragon_680_4g_mobile_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2023-33025**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3872
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3873
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3874
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3875
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3877
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3878
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3879
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3881
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3882
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3883
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3884
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3886
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3887
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3889
Product: snapdragon_685_4g_mobile_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3890
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3891
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3892
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3894
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3895
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3896
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3898
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3899
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3900
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3902
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3903
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3904
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3905
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3907
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3908
Product: snapdragon_690_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3910
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3911
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3912
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3913
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3915
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3916
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3917
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3919
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3920
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3921
Product: snapdragon_695_5g_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3922
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3923
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3924
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3925
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3927
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3928
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3929
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3931
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3932
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3933
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3934
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3936
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3937
Product: snapdragon_710_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3939
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3940
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3941
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3942
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3944
Product: snapdragon_712_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3945
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3946
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3948
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3949
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3950
Product: snapdragon_720g_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3951
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3952
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3953
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3954
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3956
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3957
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3958
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3959
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3961
Product: snapdragon_730g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3962
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3964
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3965
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3966
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3967
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3969
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3970
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3971
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_730_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3973
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3974
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3975
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3976
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-SNAP-300124/3977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3978
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3979
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3980
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3982
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3983
Product: snapdragon_732g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3985
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3986
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3987
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3988
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/3989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3990
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3991
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3992
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3993
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/3994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_750g_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3995
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3996
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3997
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-SNAP-300124/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/3999
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4000
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4002
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4003
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4004
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4005
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4007
Product: snapdragon_765g_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4008
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4009
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4011
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4012
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4013
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4015
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4016
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4017
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4019
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4020
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4021
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: snapdragon_765_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4023
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4024
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4025
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4026
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOA	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4028
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4029
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4031
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4032
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4033
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4034
Concurrent Execution using Shared Resource with Improper	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4036
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4037
Product: snapdragon_768g_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4038
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4040
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4041
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4042
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4044
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4045
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4046
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4048
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4049
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4050
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			support makes a PSCI call. **CVE ID : CVE-2023-33036**	ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4052
Product: snapdragon_778g\+_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4053
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4054
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4055
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4057
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4058
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4059
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4061
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4062
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4063
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4064
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4066
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4067
Product: snapdragon_778g_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4069
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4070
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4071
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4072
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4074
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4075
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4076
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4078
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4079
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4080
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4081
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_780g_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4083
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4084
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4085
Buffer Copy without Checking	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4087
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4088
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4089
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4091
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4092
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4093
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4094
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4096
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4097
Product: snapdragon_782g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4099
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4100
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4101
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4102
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4104
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4105
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4106
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4108
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4109
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4110
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4111
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4113
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4114
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4115
Buffer Copy without Checking	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4117
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4118
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4119
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4121
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4122
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4123
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4124
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4126
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4127
Product: snapdragon_7c_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4129
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4130
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4131
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4132
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4133
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a	https://www.qualcomm.com/c	H-QUA-SNAP-300124/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ompany/produc t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4135
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4136
Product: snapdragon_7c_gen_2_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.q ualcomm.com/c ompany/produc t-	H-QUA-SNAP-300124/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4138
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4139
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4140
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4141
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4143
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4144
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4145
Product: snapdragon_808_processor					
Affected Version(s): -					
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-SNAP-300124/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: snapdragon_810_processor					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4147
Product: snapdragon_820_automotive_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4148
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4150
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4151
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4152
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4153
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_820_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4155
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4156
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4158
Product: snapdragon_821_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4159
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4161
Product: snapdragon_835_mobile_pc_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4162
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4163
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4165
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4166
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_845_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4168
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4169
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4170
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4171
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4173
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4174
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4175
Product: snapdragon_850_mobile_compute_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4176
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4177
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4178
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4179
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4181
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4182
Product: snapdragon_855\+\/860_mobile_platform					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4184
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4185
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4186
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4187
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4189
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4190
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4191
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4192
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4194
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4195
Product: snapdragon_855_mobile_platform					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4197
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4198
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4199
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4200
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4202
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4203
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4204
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4205
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4207
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4208
Product: snapdragon_865\+_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4210
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4211
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4212
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4213
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4215
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4216
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4217
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4219
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4220
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4221
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4223
Product: snapdragon_865_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4224
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4225
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4226
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.q ualcomm.com/c	H-QUA-SNAP-300124/4227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4228
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4229
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4231
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4232
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4233
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4234
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4236
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4237
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4238
Product: snapdragon_870_5g_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4239
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4240
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4241
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4242
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4244
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4245
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4246
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4248
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4249
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4250
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4252
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4253
Product: snapdragon_888\+_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4254
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4255
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4257
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4258
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4259
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4261
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4262
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4263
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4264
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4266
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4267
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4269
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4270
Product: snapdragon_888_5g_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4271
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4272
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4274
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4275
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4276
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4278
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4279
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4280
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4281
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4283
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4284
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4285
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4287
Product: snapdragon_8cx_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4288
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4289
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4291
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4292
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4293
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4294
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4296
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4297
Product: snapdragon_8cx_gen_2_5g_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4298
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4300
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4301
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4302
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4303
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4304
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-SNAP-300124/4305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4306
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4307
Product: snapdragon_8cx_gen_3_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4309
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4310
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4311
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4313
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4314
Product: snapdragon_8c_compute_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4315
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4317
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4318
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4319
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4320
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4321
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4323
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4324
Product: snapdragon_8\+_gen_1_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4326
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4327
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4328
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4329
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4331
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4332
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4333
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4335
Product: snapdragon_8\+_gen_2_mobile_platform					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4336
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4337
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4339
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4340
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4341
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4343
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4344
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4345
Product: snapdragon_8_gen_1_mobile_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4347
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4349
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4350
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4352
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4353
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4354
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4355
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4357
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4358
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4359
Product: snapdragon_8_gen_2_mobile_platform					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4361
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4362
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4363
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4365
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4366
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4367
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4368
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-SNAP-300124/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: snapdragon_ar2_gen_1_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4370
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4371
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4372
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4374
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4375
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4376
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4378
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4379
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4380
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4382
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4383
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4384
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4385
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4387
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4388
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4389
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4391
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4393
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4394
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4396
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4397
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4399
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4400
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4401
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4402
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4404
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4405
Product: snapdragon_w5\+_gen_1_wearable_platform					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4407
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4408
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4409
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4410
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_CO	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4412
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4413
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4414
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4416
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4417
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4418
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4420
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4421
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4422
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_1300_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4424
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4425
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4426
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_2100_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4428
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4429
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4430
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_2500_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4432
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4433
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4434
Concurrent Execution using Shared Resource with	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_wear_3100_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4436
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4437
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4438
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_wear_4100\+_platform					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4440
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4441
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4443
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4444
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4446
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4447
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4448
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4449
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4451
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4452
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4453
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4455
Product: snapdragon_x20_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4456
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4458
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4459
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4460
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4462
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4463
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4464
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4465
Concurrent Execution using Shared Resource with	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4467
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4468
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4469
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4471
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4472
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4473
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4475
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4476
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4477
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4479
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4480
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4481
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4482
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4484
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4485
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4486
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4488
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4489
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4490
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4492
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4493
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4494
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: snapdragon_x5_lte_modem					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4496
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4497
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4498
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4500
Product: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4501
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4502
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4505
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4506
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4507
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4509
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4510
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4511
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4512
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4514
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4515
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4516
Product: snapdragon_x70_modem-rf_system					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4517
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4518
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4519
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4520
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4521
Concurrent Execution using Shared	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	security/bulletins/january-2024-bulletin	
Product: snapdragon_x75_5g_modem-rf_system					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4523
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4525
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4526
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4527
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4528
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: snapdragon_xr1_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4530
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4531
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4532
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4533
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-SNAP-300124/4534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4535
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4536
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.q ualcomm.com/c ompany/produc t-security/bulleti	H-QUA-SNAP-300124/4537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4538
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4539
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4540
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4542
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4543
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4544
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4545
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	H-QUA-SNAP-300124/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4547
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4548
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SNAP-300124/4549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4550
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4551
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4552
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4554
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4555
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4556
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4557
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	H-QUA-SNAP-300124/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4559
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4560
NULL Pointer Dereferenc e	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SNAP-300124/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SNAP-300124/4562
Product: ssg2115p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4563
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4564
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4565
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4567
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4568
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4569
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-SSG2-300124/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SSG2-300124/4571
Product: ssg2125p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SSG2-300124/4572
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SSG2-300124/4573
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-SSG2-300124/4574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4575
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4576
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4577
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4579
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SSG2-300124/4580
Product: sw5100					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4581
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SW51-300124/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4584
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4585
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4586
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	H-QUA-SW51-300124/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4588
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4589
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4591
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4592
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4593
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4594
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SW51-300124/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4596
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4597
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sw5100p					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4599
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4600
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4602
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	H-QUA-SW51-300124/4603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4604
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4605
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4606
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SW51-300124/4607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4608
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4609
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4610
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/c	H-QUA-SW51-300124/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4612
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4613
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4614
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SW51-300124/4615
Concurrent Execution	02-Jan-2024	7	The session index variable in PCM	https://www.qualcomm.com/c	H-QUA-SW51-300124/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ompany/product-security/bulletins/january-2024-bulletin	
Product: sxr1120					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4617
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4618
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4620
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4621
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4622
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: sxr1230p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4624
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4625
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4626
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4627
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	H-QUA-SXR1-300124/4628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4629
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4630
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR1-300124/4632
Product: sxr2130					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4633
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4634
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4635
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4637
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4638
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4639
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SXR2-300124/4640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4641
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4642
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4643
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4645
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4646
Product: sxr2230p					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4647
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4649
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4650
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4651
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4652
Concurrent Execution using Shared Resource with Improper Synchroniz	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4654
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-SXR2-300124/4655
Product: vision_intelligence_100_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4656
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-VISI-300124/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4658
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4659
Product: vision_intelligence_200_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4661
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4662
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4663
Product: vision_intelligence_300_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	H-QUA-VISI-300124/4664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4665
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4666
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4667
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4668
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-VISI-300124/4669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4670
Product: vision_intelligence_400_platform					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4671
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4672
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	H-QUA-VISI-300124/4673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4674
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4675
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4676
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-VISI-300124/4678
Product: wcd9306					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4679
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4680
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4682
Product: wcd9326					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4683
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4684
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4686
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4687
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4688
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4690
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4691
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4692
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4693
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-WCD9-300124/4694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4695
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4696
Product: wcd9330					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4698
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4699
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4700
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcd9335					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4702
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4703
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4704
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4705
Buffer Copy	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-WCD9-300124/4706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			wearables while processing data from AON. **CVE ID : CVE-2023-33085**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4707
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4708
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4709
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4711
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4712
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4713
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4715
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4716
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4717
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcd9340					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4719
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4720
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4721
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4722
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-WCD9-300124/4723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4724
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4725
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4727
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4728
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4729
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4730
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4732
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4733
Product: wcd9341					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4735
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4736
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4737
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4738
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4739
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-WCD9-300124/4740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4741
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4742
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4744
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4745
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4746
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4747
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4749
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4750
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4751
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	H-QUA-WCD9-300124/4752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Product: wcd9360					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-WCD9-300124/4753
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-WCD9-300124/4754
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-WCD9-300124/4755
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	H-QUA-WCD9-300124/4756
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.q ualcomm.com/c ompany/produc	H-QUA-WCD9-300124/4757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4758
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4759
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4760
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4762
Product: wcd9370					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4763
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4764
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4766
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4767
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4768
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4769
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4771
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4772
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4773
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	H-QUA-WCD9-300124/4774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4775
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4776
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4777
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4778
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	H-QUA-WCD9-300124/4779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4780
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4781
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4783
Product: wcd9371					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4784
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4785
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4786
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4788
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4789
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4790
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4791
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4793
Product: wcd9375					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4794
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4796
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4797
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4799
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4801
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4802
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4803
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4805
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4806
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4807
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4809
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4810
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4811
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4813
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4814
Product: wcd9380					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4815
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4817
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4818
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4820
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4822
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4823
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4824
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4826
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4827
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4828
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4829
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	H-QUA-WCD9-300124/4830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4831
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4832
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4833
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4835
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4836
Product: wcd9385					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4837
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4840
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4841
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4842
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4844
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4845
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4847
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4848
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4849
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4850
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4852
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4853
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4854
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-	H-QUA-WCD9-300124/4855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			support makes a PSCI call. **CVE ID : CVE-2023-33036**	security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4856
Product: wcd9390					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4857
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4858
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4860
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4861
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4862
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4864
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4865
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4866
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4867
Product: wcd9395					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4868
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4869
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4870
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4871
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	H-QUA-WCD9-300124/4872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4873
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4874
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4875
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-300124/4876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4877
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCD9-300124/4878
Product: wcn3610					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4879
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4881
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4882
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4883
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4885
Product: wcn3615					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4886
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4887
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4889
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4890
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4891
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-300124/4892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4893
Product: wcn3620					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4894
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4895
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-WCN3-300124/4896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4897
Product: wcn3660					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4898
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-300124/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4900
Product: wcn3660b					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4901
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4904
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4905
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4906
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-300124/4907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4908
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4909
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4911
Product: wcn3680					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4912
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4913
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4915
Product: wcn3680b					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4916
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-300124/4917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4919
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4920
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4921
Use After Free	02-Jan-2024	7.8	Memory corruption when	https://www.qualcomm.com/c	H-QUA-WCN3-300124/4922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4923
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4924
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcn3910					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4926
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4927
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4928
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4930
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4931
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4932
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	H-QUA-WCN3-300124/4933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4934
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4935
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4936
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcn3950					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4938
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4939
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4940
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4943
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4944
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4945
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECU	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4947
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4948
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4949
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-WCN3-300124/4950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4951
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4952
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4953
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4954
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-WCN3-300124/4955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4956
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4957
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33037		
Product: wcn3980					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4959
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4960
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4961
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4962
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	H-QUA-WCN3-300124/4963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4964
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4965
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4966
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4968
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4969
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4970
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-300124/4971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4972
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4973
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4974
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4975
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4977
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4978
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4979
Product: wcn3988					
Affected Version(s): -					
Buffer Copy	02-Jan-2024	9.8	Memory corruption in Data	https://www.qualcomm.com/c	H-QUA-WCN3-300124/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	ompany/product-security/bulletins/january-2024-bulletin	
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4981
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4982
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4983
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4986
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4987
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4988
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECU	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4990
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4991
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4992
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	H-QUA-WCN3-300124/4993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4994
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4995
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4996
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4997
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	H-QUA-WCN3-300124/4998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/4999
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5000
Product: wcn3990					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	H-QUA-WCN3-300124/5001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5002
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5003
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5004
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5005
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5007
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5008
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5010
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5011
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5012
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5013
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5015
Product: wcn3999					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5016
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5017
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5019
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5020
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5021
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN3-300124/5022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcn6740					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5023
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5024
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5025
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5026
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	H-QUA-WCN6-300124/5027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5028
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5029
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5030
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	H-QUA-WCN6-300124/5031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5032
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5033
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5034
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5035
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN6-300124/5036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WCN6-300124/5037
Product: wsa8810					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5038
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-300124/5039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets an IPv6 address. **CVE ID : CVE-2023-28583**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5040
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5041
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5042
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5043
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2023-33085**		
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5045
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5046
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5047
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5049
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5050
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5051
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-300124/5052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5053
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5054
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5055
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5056
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-300124/5057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5058
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5059
Product: wsa8815					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5061
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5062
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5063
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5064
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5066
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5067
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5068
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5069
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	H-QUA-WSA8-300124/5070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5071
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5072
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5074
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5075
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5076
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5077
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5079
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5080
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5081
Product: wsa8830					
Affected Version(s): -					
Buffer Copy without Checking	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP	https://www.qualcomm.com/company/product-	H-QUA-WSA8-300124/5082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			body, during a VOLTE call. **CVE ID : CVE-2023-33025**	security/bulletins/january-2024-bulletin	
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5083
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5084
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5085
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5086
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	H-QUA-WSA8-300124/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5088
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5089
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5090
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5092
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5093
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5094
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	H-QUA-WSA8-300124/5095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5096
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5097
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5098
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5099
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	H-QUA-WSA8-300124/5100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5101
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5102
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33037		
Product: wsa8832					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5104
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5105
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5106
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5107
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-300124/5108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5109
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5110
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5111
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5112
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5114
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5115
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5116
Product: wsa8835					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5117
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5118
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5119
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5120
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5122
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5123
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5124
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5125
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	H-QUA-WSA8-300124/5126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5127
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5128
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5130
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5131
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5132
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5133
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5135
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5136
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5137
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in Automotive while	https://www.qualcomm.com/company/produc	H-QUA-WSA8-300124/5138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	t-security/bulletins/january-2024-bulletin	
Product: wsa8840					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5139
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5140
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5141
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5143
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5144
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5145
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	H-QUA-WSA8-300124/5146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5147
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5148
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5149
Product: wsa8845					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5151
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5152
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5153
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5155
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5156
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5157
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5158
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-300124/5159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5160
Product: wsa8845h					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5161
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5162
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5164
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5165
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5166
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5168
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5169
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5170
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	H-QUA-WSA8-300124/5171
Vendor: Tenda					
Product: a18					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Jan-2024	9.8	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2023-50585**	N/A	H-TEN-A18-300124/5172
Product: ax12					
Affected Version(s): -					
Out-of-bounds Write	10-Jan-2024	7.5	Buffer Overflow vulnerability in Tenda AX12 V22.03.01.46, allows remote attackers to cause a denial of service (DoS) via list parameter in SetNetControlList function. **CVE ID : CVE-2023-49427**	N/A	H-TEN-AX12-300124/5173
Product: ax1803					
Affected Version(s): -					
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function getIptvInfo. **CVE ID : CVE-2023-51971**	N/A	H-TEN-AX18-300124/5174
Improper Neutralization of	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 was discovered to	N/A	H-TEN-AX18-300124/5175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			contain a command injection vulnerability via the function fromAdvSetLanIp. **CVE ID : CVE-2023-51972**		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formGetIptv. **CVE ID : CVE-2023-51961**	N/A	H-TEN-AX18-300124/5176
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo. **CVE ID : CVE-2023-51966**	N/A	H-TEN-AX18-300124/5177
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formSetIptv. **CVE ID : CVE-2023-51952**	N/A	H-TEN-AX18-300124/5178
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode	N/A	H-TEN-AX18-300124/5179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in the function formSetIptv. **CVE ID : CVE-2023-51953**		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formSetIptv. **CVE ID : CVE-2023-51954**	N/A	H-TEN-AX18-300124/5180
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formSetIptv. **CVE ID : CVE-2023-51955**	N/A	H-TEN-AX18-300124/5181
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formSetIptv **CVE ID : CVE-2023-51956**	N/A	H-TEN-AX18-300124/5182
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv.	N/A	H-TEN-AX18-300124/5183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51957		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv. **CVE ID : CVE-2023-51958**	N/A	H-TEN-AX18-300124/5184
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv. **CVE ID : CVE-2023-51959**	N/A	H-TEN-AX18-300124/5185
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv. **CVE ID : CVE-2023-51960**	N/A	H-TEN-AX18-300124/5186
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo. **CVE ID : CVE-2023-51963**	N/A	H-TEN-AX18-300124/5187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo. **CVE ID : CVE-2023-51964**	N/A	H-TEN-AX18-300124/5188
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo. **CVE ID : CVE-2023-51965**	N/A	H-TEN-AX18-300124/5189
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo. **CVE ID : CVE-2023-51962**	N/A	H-TEN-AX18-300124/5190
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function getIptvInfo. **CVE ID : CVE-2023-51967**	N/A	H-TEN-AX18-300124/5191
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the	N/A	H-TEN-AX18-300124/5192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adv.iptv.stballvlans parameter in the function getIptvInfo. **CVE ID : CVE-2023-51968**		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function getIptvInfo. **CVE ID : CVE-2023-51969**	N/A	H-TEN-AX18-300124/5193
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv. **CVE ID : CVE-2023-51970**	N/A	H-TEN-AX18-300124/5194
Product: ax3					
Affected Version(s): -					
N/A	04-Jan-2024	9.8	Tenda AX3 v16.03.12.11 was discovered to contain a remote code execution (RCE) vulnerability via the list parameter at /goform/SetNetControlList. **CVE ID : CVE-2023-51812**	N/A	H-TEN-AX3-300124/5195
Product: i29					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.5	Buffer Overflow vulnerability in Tenda i29 versions 1.0 V1.0.0.5 and 1.0 V1.0.0.2, allows remote attackers to cause a denial of service (DoS) via the pingIp parameter in the pingSet function. **CVE ID : CVE-2023-50991**	N/A	H-TEN-I29-300124/5196
Vendor: totolink					
Product: lr1200gb					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249858 is the identifier assigned to this vulnerability.	N/A	H-TOT-LR12-300124/5197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0292**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this vulnerability is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249859. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0293**	N/A	H-TOT-LR12-300124/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this issue is the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249860. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0294**	N/A	H-TOT-LR12-300124/5199
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. This affects the function	N/A	H-TOT-LR12-300124/5200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249861 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0295**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jan-2024	8.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to command injection. The attack may be	N/A	H-TOT-LR12-300124/5201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249857 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0291**		
Product: n200re					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249862 is the identifier assigned	N/A	H-TOT-N200-300124/5202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249863. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TOT-N200-300124/5203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0297		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. Affected is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command 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-249864. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0298**	N/A	H-TOT-N200-300124/5204
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. Affected by this vulnerability is the function	N/A	H-TOT-N200-300124/5205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249865 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0299**		
Product: n350rt					
Affected Version(s): -					
Stack-based Buffer Overflow	09-Jan-2024	9.8	A vulnerability has been found in Totolink N350RT 9.3.5u.6139_B202012 and classified as critical. Affected by this vulnerability is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer	N/A	H-TOT-N350-300124/5206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7219**		
Out-of-bounds Write	07-Jan-2024	8.8	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this vulnerability is the function main of the file /cgi-bin/cstecgi.cgi?action=login&flag=1 of the component HTTP POST Request Handler. The manipulation of the argument v33 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may	N/A	H-TOT-N350-300124/5207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier VDB-249769 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7213**		
Out-of-bounds Write	07-Jan-2024	8.8	A vulnerability, which was classified as critical, has been found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this issue is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v8 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249770 is the identifier assigned to this vulnerability.	N/A	H-TOT-N350-300124/5208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7214**		
Stack-based Buffer Overflow	08-Jan-2024	7.2	A vulnerability, which was classified as critical, was found in Totolink N350RT 9.3.5u.6139_B202012. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-249852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7218**	N/A	H-TOT-N350-300124/5209
Product: nr1800x					
Affected Version(s): -					
Stack-based	09-Jan-2024	9.8	A vulnerability was found in Totolink	N/A	H-TOT-NR18-300124/5210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			NR1800X 9.1.0u.6279_B20210910 and classified as critical. Affected by this issue is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249854 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-2023-7220**		
Product: t6					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Jan-2024	9.8	A vulnerability was found in Totolink T6 4.1.9cu.5241_B20210923. It has been classified as critical. This affects the function main of the file /cgi-bin/cstecgi.cgi?acti	N/A	H-TOT-T6-300124/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on=login of the component HTTP POST Request Handler. The manipulation of the argument v41 leads to buffer overflow. 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-249855. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7221**		
Improper Access Control	09-Jan-2024	6.5	A vulnerability classified as problematic has been found in Totolink T6 4.1.9cu.5241_B20210923. This affects an unknown part of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument topicurl with the input showSyslog leads to improper access controls. It is	N/A	H-TOT-T6-300124/5212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-249867. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7223**		
Product: x2000r					
Affected Version(s): -					
Out-of-bounds Write	09-Jan-2024	9.8	A vulnerability was found in Totolink X2000R 1.0.0-B20221212.1452. It has been declared as critical. This vulnerability affects the function formTmultiAP of the file /bin/boa of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may	N/A	H-TOT-X200-300124/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier of this vulnerability is VDB-249856. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7222**		
Affected Version(s): v2					
Out-of-bounds Write	07-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink X2000R_V2 2.0.0-B20230727.10434. This vulnerability affects the function formTmultiAP of the file /bin/boa. The manipulation leads to buffer overflow. VDB-249742 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-2023-7208**	N/A	H-TOT-X200-300124/5214
Vendor: Tp-link					
Product: tapo_c200					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	09-Jan-2024	7.5	TP-Link Tapo APK up to v2.12.703 uses hardcoded credentials for access to the login panel. **CVE ID : CVE-2023-27098**	N/A	H-TP--TAPO-300124/5215
Vendor: Trendnet					
Product: tv-ip1314pi					
Affected Version(s): -					
N/A	09-Jan-2024	9.8	An issue was discovered in libremote_dbg.so on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Filtering of debug information is mishandled during use of popen. Consequently, an attacker can bypass validation and execute a shell command. **CVE ID : CVE-2023-49235**	https://drive.google.com/file/d/1lTloBkH_7zAz1ZbFVSZnfpoPd81aPaHx/view?usp=sharing	H-TRE-TV-I-300124/5216
Out-of-bounds Write	09-Jan-2024	9.8	A stack-based buffer overflow was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices, leading to arbitrary command execution. This occurs because of lack of length validation during an sscanf of a user-entered scale field	https://drive.google.com/file/d/1lTloBkH_7zAz1ZbFVSZnfpoPd81aPaHx/view?usp=sharing	H-TRE-TV-I-300124/5217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the RTSP playback function of davinci. **CVE ID : CVE-2023-49236**		
Vendor: uniwayinfo					
Product: uw-101x					
Affected Version(s): -					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-UNI-UW-1-300124/5218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**	N/A	H-UNI-UW-1-300124/5219
Product: uw-301vpw					
Affected Version(s): -					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has	N/A	H-UNI-UW-3-300124/5220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the	N/A	H-UNI-UW-3-300124/5221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**		
Product: uw-302vp					
Affected Version(s): -					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be	N/A	H-UNI-UW-3-300124/5222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-	N/A	H-UNI-UW-3-300124/5223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			249758 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-2023-7209**		
Product: uw-311vpw					
Affected Version(s): -					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 is the identifier assigned to this	N/A	H-UNI-UW-3-300124/5224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**	N/A	H-UNI-UW-3-300124/5225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uw-323dac					
Affected Version(s): -					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**	N/A	H-UNI-UW-3-300124/5226
Improper Resource	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It	N/A	H-UNI-UW-3-300124/5227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**		
Vendor: ZTE					
Product: red_magic_8_pro					
Affected Version(s): -					
N/A	04-Jan-2024	5.5	Permissions and Access Control Vulnerability in ZTE Red Magic 8 Pro **CVE ID : CVE-2023-41784**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034444	H-ZTE-RED_-300124/5228
Product: zxcloud_irai					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	03-Jan-2024	7.8	There is a local privilege escalation vulnerability of ZTE's ZXCLOUD iRAI.Attackers with regular user privileges can create a fake process, and to escalate local privileges. **CVE ID : CVE-2023-41776**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	H-ZTE-ZXCL-300124/5229
Uncontrolled Search Path Element	03-Jan-2024	7.8	There is an unsafe DLL loading vulnerability in ZTE ZXCLOUD iRAI. Due to the program failed to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges. **CVE ID : CVE-2023-41780**	https://https//support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	H-ZTE-ZXCL-300124/5230
Improper Control of Generation of Code ('Code Injection')	03-Jan-2024	7.8	There is a command injection vulnerability of ZTE's ZXCLOUD iRAI. Due to the program failed to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges.	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	H-ZTE-ZXCL-300124/5231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41783		
Incorrect Authorization	03-Jan-2024	5.5	There is an illegal memory access vulnerability of ZTE's ZXCLOUD iRAI product.When the vulnerability is exploited by an attacker with the common user permission, the physical machine will be crashed. **CVE ID : CVE-2023-41779**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	H-ZTE-ZXCL-300124/5232
Uncontrolled Search Path Element	05-Jan-2024	4.8	There is a DLL hijacking vulnerability in ZTE ZXCLOUD iRAI, an attacker could place a fake DLL file in a specific directory and successfully exploit this vulnerability to execute malicious code. **CVE ID : CVE-2023-41782**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1032984	H-ZTE-ZXCL-300124/5233
Operating System					
Vendor: ami					
Product: megarac_sp-x					
Affected Version(s): From (including) 12 Up to (excluding) 12.7					
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI	O-AMI-MEGA-310124/5234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37293**	-SA-2023010.pdf	
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37294**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5235
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37295**		
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37296**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5237
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37297**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-3043**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5239
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jan-2024	7.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference by a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-34332**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5240
Improper Restriction of Operations within the Bounds of	09-Jan-2024	7.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security	O-AMI-MEGA-310124/5241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			dereference via a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-34333**	Advisories/AMI-SA-2023010.pdf	
Affected Version(s): From (including) 13 Up to (excluding) 13.6					
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37293**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5242
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37294**		
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37295**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5244
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability. **CVE ID : CVE-2023-37296**		
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-37297**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5246
Out-of-bounds Write	09-Jan-2024	8.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-3043**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jan-2024	7.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference by a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-34332**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5248
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Jan-2024	7.8	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference via a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability. **CVE ID : CVE-2023-34333**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security Advisories/AMI-SA-2023010.pdf	O-AMI-MEGA-310124/5249
Vendor: Apple					
Product: macos					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20710**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-APP-MACO-310124/5250
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20711**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-APP-MACO-310124/5251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20712**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-APP-MACO-310124/5252
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20713**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-APP-MACO-310124/5253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.0					
N/A	10-Jan-2024	7.8	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to arbitrary code execution. **CVE ID : CVE-2023-42826**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5254
N/A	10-Jan-2024	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to gain elevated privileges. **CVE ID : CVE-2023-42933**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5255
N/A	10-Jan-2024	7.1	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to a denial-of-service or potentially disclose memory contents. **CVE ID : CVE-2023-42876**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5256
N/A	10-Jan-2024	5.5	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14. An app may be able	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access user-sensitive data. **CVE ID : CVE-2023-40411**		
N/A	10-Jan-2024	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access removable volumes without user consent. **CVE ID : CVE-2023-40430**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5258
N/A	10-Jan-2024	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41987**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5259
N/A	10-Jan-2024	5.5	A logic issue was addressed with improved checks This issue is fixed in macOS Sonoma 14. A camera extension may be able to access the camera view from apps other than the app for which it was granted permission. **CVE ID : CVE-2023-41994**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access protected user data. **CVE ID : CVE-2023-42929**	https://support.apple.com/en-us/HT213940	O-APP-MACO-310124/5261
Vendor: autelrobotics					
Product: evo_nano_drone_firmware					
Affected Version(s): 1.6.5					
N/A	06-Jan-2024	5.7	Autel EVO NANO drone flight control firmware version 1.6.5 is vulnerable to denial of service (DoS). **CVE ID : CVE-2023-50121**	N/A	O-AUT-EVO_-310124/5262
Vendor: automaticsystems					
Product: soc_fl9600_firstlane_firmware					
Affected Version(s): 06					
Use of Hard-coded Credentials	03-Jan-2024	7.5	An issue in Automatic Systems SOC FL9600 FastLine v.lego_T04E00 allows a remote attacker to obtain sensitive information via the admin login credentials. **CVE ID : CVE-2023-37608**	N/A	O-AUT-SOC_-310124/5263
Improper Limitation	03-Jan-2024	7.5	Directory Traversal in Automatic-	N/A	O-AUT-SOC_-310124/5264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Systems SOC FL9600 FastLine lego_T04E00 allows a remote attacker to obtain sensitive information. **CVE ID : CVE-2023-37607**		
Vendor: byzoro					
Product: smart_s150_firmware					
Affected Version(s): * Up to (including) 2024-01-01					
Unrestricted Upload of File with Dangerous Type	08-Jan-2024	9.8	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform up to 20240101. It has been rated as critical. Affected by this issue is some unknown functionality of the file /useratte/useratteStation.php of the component HTTP POST Request Handler. The manipulation of the argument web_img leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249866 is the identifier assigned to this	N/A	O-BYZ-SMAR-310124/5265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0300**		
Vendor: Canonical					
Product: ubuntu_linux					
Affected Version(s): 14.04					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t	O-CAN-UBUN-310124/5266
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0. **CVE ID : CVE-2022-2588**	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-CAN-UBUN-310124/5267
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d9	O-CAN-UBUN-310124/5268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	50da74bb2bd90	
Affected Version(s): 16.04					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t	O-CAN-UBUN-310124/5269
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0. **CVE ID : CVE-2022-2588**	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-CAN-UBUN-310124/5270
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d9	O-CAN-UBUN-310124/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	50da74bb2bd90	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	O-CAN-UBUN-310124/5272
Affected Version(s): 18.04					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t	O-CAN-UBUN-310124/5273
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-CAN-UBUN-310124/5274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			its handle had the value 0. **CVE ID : CVE-2022-2588**		
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-CAN-UBUN-310124/5275
Use After Free	08-Jan-2024	7	io_uring UAF, Unix SCM garbage collection **CVE ID : CVE-2022-2602**	N/A	O-CAN-UBUN-310124/5276
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	O-CAN-UBUN-310124/5277
Affected Version(s): 20.04					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set	https://lore.kernel.org/netfilter-devel/2022080	O-CAN-UBUN-310124/5278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	9170148.164591-1-cascardo@canonical.com/T/#t	
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0. **CVE ID : CVE-2022-2588**	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-CAN-UBUN-310124/5279
Use After Free	08-Jan-2024	7	io_uring UAF, Unix SCM garbage collection **CVE ID : CVE-2022-2602**	N/A	O-CAN-UBUN-310124/5280
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	O-CAN-UBUN-310124/5281
Affected Version(s): 22.04					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set	https://lore.kernel.org/netfilter-devel/2022080	O-CAN-UBUN-310124/5282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	9170148.164591-1-cascardo@canonical.com/T/#t	
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0. **CVE ID : CVE-2022-2588**	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-CAN-UBUN-310124/5283
Use After Free	08-Jan-2024	7	io_uring UAF, Unix SCM garbage collection **CVE ID : CVE-2022-2602**	N/A	O-CAN-UBUN-310124/5284
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	O-CAN-UBUN-310124/5285
Double Free	08-Jan-2024	5.5	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function	N/A	O-CAN-UBUN-310124/5286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067. **CVE ID : CVE-2023-1032**		
Affected Version(s): 22.10					
Use After Free	08-Jan-2024	7	io_uring UAF, Unix SCM garbage collection **CVE ID : CVE-2022-2602**	N/A	O-CAN-UBUN-310124/5287
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2024	7	Race condition in snap-confine's must_mkdir_and_open_with_perms() **CVE ID : CVE-2022-3328**	https://ubuntu.com/security/notices/USN-5753-1	O-CAN-UBUN-310124/5288
Double Free	08-Jan-2024	5.5	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1	N/A	O-CAN-UBUN-310124/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067. **CVE ID : CVE-2023-1032**		
Vendor: Dlink					
Product: r15_firmware					
Affected Version(s): * Up to (including) 1.08.02					
N/A	10-Jan-2024	5.3	D-Link R15 before v1.08.02 was discovered to contain no firewall restrictions for IPv6 traffic. This allows attackers to arbitrarily access any services running on the device that may be inadvertently listening via IPv6. **CVE ID : CVE-2023-41603**	https://support announcement.us.dlink.com/announcement/publication.aspx?name=SAP10347	O-DLI-R15_-310124/5290
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 34					
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-FED-FEDO-310124/5291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code. **CVE ID : CVE-2021-3600**		
Affected Version(s): 38					
Use After Free	04-Jan-2024	8.8	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 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-2024-0222**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html, https://crbug.com/1501798	O-FED-FEDO-310124/5292
Out-of-bounds Write	04-Jan-2024	8.8	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0223**	https://crbug.com/1505009	O-FED-FEDO-310124/5293
Use After Free	04-Jan-2024	8.8	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199	https://crbug.com/1505086	O-FED-FEDO-310124/5294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0224**		
Use After Free	04-Jan-2024	8.8	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0225**	https://crbug.com/1506923	O-FED-FEDO-310124/5295
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	7.8	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter.	https://access.redhat.com/security/cve/CVE-2023-6004, https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LZQVUHWVWRH73YBXUQJOD6CKHDQBU3DM/	O-FED-FEDO-310124/5296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6004		
Affected Version(s): 39					
Use After Free	04-Jan-2024	8.8	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 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-2024-0222**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html, https://crbug.com/1501798	O-FED-FEDO-310124/5297
Out-of-bounds Write	04-Jan-2024	8.8	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0223**	https://crbug.com/1505009	O-FED-FEDO-310124/5298
Use After Free	04-Jan-2024	8.8	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to	https://crbug.com/1505086	O-FED-FEDO-310124/5299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0224**		
Use After Free	04-Jan-2024	8.8	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0225**	https://crbug.com/1506923	O-FED-FEDO-310124/5300
Use After Free	04-Jan-2024	7	A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition	N/A	O-FED-FEDO-310124/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or potential code execution. **CVE ID : CVE-2023-6270**		
Vendor: geniecompany					
Product: aladdin_connect_garage_door_opener_firmware					
Affected Version(s): * Up to (including) 14.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Jan-2024	8.8	When the Genie Company Aladdin Connect garage door opener (Retrofit-Kit Model ALDCM) is placed into configuration mode the web servers "Garage Door Control Module Setup" page is vulnerable to XSS via a broadcast SSID name containing malicious code with client side Java Script and/or HTML. This allows the attacker to inject malicious code with client side Java Script and/or HTML into the users' web browser. **CVE ID : CVE-2023-5880**	https://www.rapid7.com/blog/post/2024/01/03/genie-aladdin-connect-retrofit-garage-door-opener-multiple-vulnerabilities/	O-GEN-ALAD-310124/5302
Missing Authentication for Critical Function	03-Jan-2024	8.2	Unauthenticated access permitted to web interface page The Genie Company Aladdin Connect (Retrofit-	https://www.rapid7.com/blog/post/2024/01/03/genie-aladdin-connect-	O-GEN-ALAD-310124/5303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kit Model ALDCM) "Garage Door Control Module Setup" and modify the Garage door's SSID settings. **CVE ID : CVE-2023-5881**	retrofit-garage-door-opener-multiple-vulnerabilities/	
Vendor: gl-inet					
Product: gl-a1300_firmware					
Affected Version(s): 4.4.6					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-A-310124/5304
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken	N/A	O-GL--GL-A-310124/5305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-ar300m_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7,	N/A	O-GL--GL-A-310124/5306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	O-GL--GL-A-310124/5307
Product: gl-ar750s_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the	N/A	O-GL--GL-A-310124/5308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7,	N/A	O-GL--GL-A-310124/5309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-ar750_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-A-310124/5310
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific	N/A	O-GL--GL-A-310124/5311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-ax1800_firmware					
Affected Version(s): 4.4.6					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	N/A	O-GL--GL-A-310124/5312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50921		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	O-GL--GL-A-310124/5313
Product: gl-axt1800_firmware					
Affected Version(s): 4.4.6					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root	N/A	O-GL--GL-A-310124/5314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	N/A	O-GL--GL-A-310124/5315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50922		
Product: gl-b1300_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-B-310124/5316
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its	N/A	O-GL--GL-B-310124/5317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-mt1300_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-M-310124/5318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	O-GL--GL-M-310124/5319
Product: gl-mt2500_firmware					
Affected Version(s): 4.4.6					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6,	N/A	O-GL--GL-M-310124/5320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	O-GL--GL-M-310124/5321
Product: gl-mt3000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.4.6					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-M-310124/5322
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6,	N/A	O-GL--GL-M-310124/5323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-mt300n-v2_firmware					
Affected Version(s): 4.3.7					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**	N/A	O-GL--GL-M-310124/5324
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are	N/A	O-GL--GL-M-310124/5325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**		
Product: gl-mt6000_firmware					
Affected Version(s): 4.5.0					
N/A	03-Jan-2024	9.8	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7,	N/A	O-GL--GL-M-310124/5326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50921**		
Unrestricted Upload of File with Dangerous Type	03-Jan-2024	7.2	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7. **CVE ID : CVE-2023-50922**	N/A	O-GL--GL-M-310124/5327
Vendor: Google					
Product: android					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	02-Jan-2024	5.5	There is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of health data with no additional execution privileges needed. **CVE ID : CVE-2023-4164**	https://source.android.com/docs/security/bulletin/pixel-watch/2023/2023-12-01	O-GOO-ANDR-310124/5328
Affected Version(s): 11.0					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5329
Out-of-bounds Write	02-Jan-2024	6.7	In keyInstall, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	O-GOO-ANDR-310124/5330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5331
Out-of-bounds Read	02-Jan-2024	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/January-2024	O-GOO-ANDR-310124/5332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5333
Affected Version(s): 12.0					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**		
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5335
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308070.	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32877		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5337
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5338
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing	https://corp.mediatek.com/product-security-	O-GOO-ANDR-310124/5339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	bulletin/January-2024	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5340
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**		
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5342
Out-of-bounds Read	02-Jan-2024	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: ALPS08308607;	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5344
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5346
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5347
Affected Version(s): 13.0					
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of	https://corp.mediatek.com/product-security-	O-GOO-ANDR-310124/5348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895). **CVE ID : CVE-2023-32889**	bulletin/January-2024	
Out-of-bounds Write	02-Jan-2024	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: ALPS08308607; Issue ID: ALPS08308607. **CVE ID : CVE-2023-32872**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5349
Out-of-bounds Write	02-Jan-2024	6.7	In battery, 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/January-2024	O-GOO-ANDR-310124/5350

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: ALPS08308070; Issue ID: ALPS08308070. **CVE ID : CVE-2023-32877**		
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308064. **CVE ID : CVE-2023-32879**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5351
Out-of-bounds Write	02-Jan-2024	6.7	In battery, there is a possible memory corruption due to a 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/January-2024	O-GOO-ANDR-310124/5352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS08308070; Issue ID: ALPS08308616. **CVE ID : CVE-2023-32882**		
Out-of-bounds Write	02-Jan-2024	6.7	In Engineer Mode, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08282249; Issue ID: ALPS08282249. **CVE ID : CVE-2023-32883**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5353
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011. **CVE ID : CVE-2023-32884**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	6.7	In display drm, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780685; Issue ID: ALPS07780685. **CVE ID : CVE-2023-32885**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5355
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559. **CVE ID : CVE-2023-32891**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5356
Out-of-bounds Read	02-Jan-2024	4.4	In keyInstall, there is a possible information disclosure due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5357

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: ALPS08308607; Issue ID: ALPS08304217. **CVE ID : CVE-2023-32875**		
Out-of-bounds Read	02-Jan-2024	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: ALPS08308612; Issue ID: ALPS08308612. **CVE ID : CVE-2023-32876**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5358
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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/January-2024	O-GOO-ANDR-310124/5359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08307992. **CVE ID : CVE-2023-32878**		
Out-of-bounds Read	02-Jan-2024	4.4	In battery, 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: ALPS08308070; Issue ID: ALPS08308076. **CVE ID : CVE-2023-32880**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5360
Integer Overflow or Wraparound	02-Jan-2024	4.4	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070;	https://corp.mediatek.com/product-security-bulletin/January-2024	O-GOO-ANDR-310124/5361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS08308080. **CVE ID : CVE-2023-32881**		
Product: home_firmware					
Affected Version(s): * Up to (excluding) 2.58					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	O-GOO-HOME-310124/5362
Product: home_mini_firmware					
Affected Version(s): * Up to (excluding) 2.58					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	O-GOO-HOME-310124/5363
Product: nest_audio_firmware					
Affected Version(s): * Up to (excluding) 2.58					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021	O-GOO-NEST-310124/5364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege **CVE ID : CVE-2023-48419**	&sjid=4533873659772963473-NA#zippy=%2Cspeakers	
Product: nest_mini_firmware					
Affected Version(s): * Up to (excluding) 2.58					
N/A	02-Jan-2024	9.8	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege **CVE ID : CVE-2023-48419**	https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers	O-GOO-NEST-310124/5365
Product: nest_wifi_pro_firmware					
Affected Version(s): -					
Missing Encryption of Sensitive Data	02-Jan-2024	9.8	Google Nest WiFi Pro root code-execution & user-data compromise **CVE ID : CVE-2023-6339**	N/A	O-GOO-NEST-310124/5366
Product: pixel_watch_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.8	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default	https://source.android.com/docs/security/bulletin/pixel-watch/2023/2023-12-01	O-GOO-PIXE-310124/5367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation **CVE ID : CVE-2023-48418**		
Vendor: hitachienergy					
Product: relion_650_firmware					
Affected Version(s): 2.2.0					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package.	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Affected Version(s): 2.2.1					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Affected Version(s): 2.2.4					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service.	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3864		
Affected Version(s): 2.2.5					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5371
Product: relion_670_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.2.0					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5372
Affected Version(s): 2.2.1					
Improper Verification of	04-Jan-2024	4.5	A vulnerability exists in the Relion	https://publisher.hitachienergy.com/preview?	O-HIT-RELI-310124/5373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	
Affected Version(s): 2.2.4					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPart	O-HIT-RELI-310124/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**	Id=&Action=Launch	
Affected Version(s): 2.2.5					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Affected Version(s): 2.2.2					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Affected Version(s): 2.2.3					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Product: relion_sam600-io_firmware					
Affected Version(s): 2.2.1					
Improper Verification of Cryptographic Signature	04-Jan-2024	4.5	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000146&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RELI-310124/5378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service. **CVE ID : CVE-2022-3864**		
Product: rtu520_firmware					
Affected Version(s): 13.3.1					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.0.1 Up to (including) 12.0.13					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5380
Affected Version(s): From (including) 12.2.1 Up to (including) 12.2.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5381
Affected Version(s): From (including) 12.4.1 Up to (including) 12.4.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.6.1 Up to (including) 12.6.7					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.7.1 Up to (including) 12.7.3					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5384
Affected Version(s): From (including) 13.2.1 Up to (including) 13.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5385
Product: rtu530_firmware					
Affected Version(s): 13.3.1					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.0.1 Up to (including) 12.0.13					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.2.1 Up to (including) 12.2.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 12.4.1 Up to (including) 12.4.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5389
Affected Version(s): From (including) 12.6.1 Up to (including) 12.6.7					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.7.1 Up to (including) 12.7.3					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 13.2.1 Up to (including) 13.2.4					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rtu540_firmware					
Affected Version(s): 13.3.1					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5393
Affected Version(s): From (including) 12.0.1 Up to (including) 12.0.13					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPart	O-HIT-RTU5-310124/5394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	Id=&Action=Launch	
Affected Version(s): From (including) 12.2.1 Up to (including) 12.2.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.4.1 Up to (including) 12.4.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function.	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2081		
Affected Version(s): From (including) 12.6.1 Up to (including) 12.6.7					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5397
Affected Version(s): From (including) 12.7.1 Up to (including) 12.7.3					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPart	O-HIT-RTU5-310124/5398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	Id=&Action=Launch	
Affected Version(s): From (including) 13.2.1 Up to (including) 13.2.4					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Product: rtu560_firmware					
Affected Version(s): 13.3.1					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.0.1 Up to (including) 12.0.13					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5401
Affected Version(s): From (including) 12.2.1 Up to (including) 12.2.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&La	O-HIT-RTU5-310124/5402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	nguageCode=en&DocumentPartId=&Action=Launch	
Affected Version(s): From (including) 12.4.1 Up to (including) 12.4.11					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.6.1 Up to (including) 12.6.7					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modbus TCP function. **CVE ID : CVE-2022-2081**		
Affected Version(s): From (including) 12.7.1 Up to (including) 12.7.3					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&LanguageCode=en&DocumentPartId=&Action=Launch	O-HIT-RTU5-310124/5405
Affected Version(s): From (including) 13.2.1 Up to (including) 13.2.4					
Out-of-bounds Write	04-Jan-2024	7.5	A vulnerability exists in the HCI Modbus TCP function included in the product	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000111&La	O-HIT-RTU5-310124/5406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function. **CVE ID : CVE-2022-2081**	nguageCode=en&DocumentPartId=&Action=Launch	
Vendor: Infoblox					
Product: nios					
Affected Version(s): 8.5.2-409296					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Jan-2024	5.4	A stored cross-site scripting (XSS) vulnerability in Infoblox NIOS v8.5.2-409296 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the VLAN View Name field.	N/A	O-INF-NIOS-310124/5407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28975		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Use After Free	04-Jan-2024	7	A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or potential code execution. **CVE ID : CVE-2023-6270**	N/A	O-LIN-LINU-310124/5408
Use After Free	02-Jan-2024	6.7	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-collected when the pipapo set is removed, the element can be deactivated twice. This can cause a	https://bugzilla.redhat.com/show_bug.cgi?id=2255653	O-LIN-LINU-310124/5409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free issue on an NFT_CHAIN object or NFT_OBJECT object, allowing a local unprivileged user with CAP_NET_ADMIN capability to escalate their privileges on the system. **CVE ID : CVE-2024-0193**		
Affected Version(s): * Up to (excluding) 5.10					
Uncontrolled Resource Consumption	05-Jan-2024	4.9	Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other	https://xenbits.xenproject.org/xsa/advisory-441.html	O-LIN-LINU-310124/5410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock). **CVE ID : CVE-2023-34324**		
Affected Version(s): * Up to (excluding) 6.3					
Missing Release of Memory after Effective Lifetime	02-Jan-2024	4.4	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to	https://bugzilla.redhat.com/show_bug.cgi?id=2256279, https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=ac4893980bbe79ce383daf9a0885666a30fe4c83	O-LIN-LINU-310124/5411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a refcount overflow. **CVE ID : CVE-2023-7192**		
Affected Version(s): * Up to (including) 5.19.17					
Use After Free	08-Jan-2024	7.8	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted. **CVE ID : CVE-2022-2586**	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t	O-LIN-LINU-310124/5412
Double Free	08-Jan-2024	7.8	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0. **CVE ID : CVE-2022-2588**	https://lore.kernel.org/netdev/20220809170518.164662-1-cascardo@canonical.com/T/#u	O-LIN-LINU-310124/5413
Affected Version(s): * Up to (including) 6.0.19					
Use After Free	08-Jan-2024	7	io_uring UAF, Unix SCM garbage collection **CVE ID : CVE-2022-2602**	N/A	O-LIN-LINU-310124/5414
Affected Version(s): 5.11					
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d9	O-LIN-LINU-310124/5415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	50da74bb2bd90	
Affected Version(s): 6.3					
Double Free	08-Jan-2024	5.5	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067. **CVE ID : CVE-2023-1032**	N/A	O-LIN-LINU-310124/5416
Affected Version(s): From (including) 4.14 Up to (excluding) 4.19.206					
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-LIN-LINU-310124/5417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.98					
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-LIN-LINU-310124/5418
Affected Version(s): From (including) 5.19 Up to (excluding) 6.3					
Double Free	08-Jan-2024	5.5	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067.	N/A	O-LIN-LINU-310124/5419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1032		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.16					
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-LIN-LINU-310124/5420
Vendor: mediatek					
Product: lr13					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-LR13-310124/5421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-LR13-310124/5422
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-LR13-310124/5423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: nr15					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5424
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5426
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5428
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR15-310124/5429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: nr16					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5430
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5432
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5434
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR16-310124/5435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: nr17					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	9.8	In Modem IMS Stack, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161803; Issue ID: MOLY01161803 (MSV-893). **CVE ID : CVE-2023-32874**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5436
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS SMS UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MOLY00730807; Issue ID: MOLY00730807. **CVE ID : CVE-2023-32886**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Jan-2024	7.5	In Modem IMS Stack, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161837; Issue ID: MOLY01161837 (MSV-892). **CVE ID : CVE-2023-32887**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5438
Out-of-bounds Write	02-Jan-2024	7.5	In Modem IMS Call UA, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01161830;	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: MOLY01161830 (MSV-894). **CVE ID : CVE-2023-32888**		
Improper Input Validation	02-Jan-2024	7.5	In modem EMM, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01183647; Issue ID: MOLY01183647 (MSV-963). **CVE ID : CVE-2023-32890**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5440
Out-of-bounds Write	02-Jan-2024	6.7	In bluetooth 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: ALPS07933038; Issue ID: MSV-559.	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-NR17-310124/5441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32891		
Product: software_development_kit					
Affected Version(s): * Up to (including) 7.6.7.1					
Use of Insufficiently Random Values	02-Jan-2024	5.5	In wlan driver, there is a possible PIN crack due to use of insufficiently random values. This could lead to local information disclosure with no execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00325055; Issue ID: MSV-868. **CVE ID : CVE-2023-32831**	https://corp.mediatek.com/product-security-bulletin/January-2024	O-MED-SOFT-310124/5442
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	A vulnerability was found in Perl. This security issue occurs while Perl for Windows relies on the system path environment variable to find the shell (`cmd.exe`). When running an executable that uses the Windows Perl interpreter, Perl attempts to find and execute `cmd.exe` within	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1056746	O-MIC-WIND-310124/5443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the operating system. However, due to path search order issues, Perl initially looks for cmd.exe in the current working directory. This flaw allows an attacker with limited privileges to place`cmd.exe` in locations with weak permissions, such as `C:\ProgramData`. By doing so, arbitrary code can be executed when an administrator attempts to use this executable from these compromised locations. **CVE ID : CVE-2023-47039**		
N/A	07-Jan-2024	7.8	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402. **CVE ID : CVE-2023-47145**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270402, https://www.ibm.com/support/pages/node/7105500	O-MIC-WIND-310124/5444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20710**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-MIC-WIND-310124/5445
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20711**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-MIC-WIND-310124/5446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20712**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-MIC-WIND-310124/5447
Out-of-bounds Read	10-Jan-2024	5.5	Adobe Substance 3D Stager versions 2.1.3 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-2024-20713**	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-06.html	O-MIC-WIND-310124/5448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20402					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5449
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5450
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5451
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5452
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5453
Concurrent Execution using Shared Resource with Improper	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')					
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5455
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5456
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5457
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5458
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5459
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-21314**	guide/vulnerability/CVE-2024-21314	
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5461
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5462
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5463
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5464
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5465
Product: windows_10_1607					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5466
Affected Version(s): * Up to (excluding) 10.0.14393.6614					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5467
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5468
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5469
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5470
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5471
Concurrent Execution	09-Jan-2024	7.5	Remote Desktop Client Remote Code	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2024-21307**	date-guide/vulnerability/CVE-2024-21307	
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5473
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5474
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5475
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5476
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20680	lity/CVE-2024-20680	
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5478
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5479
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5480
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5481
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5482
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-21311**	lity/CVE-2024-21311	
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5484
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5485
Product: windows_10_1809					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5486
Affected Version(s): * Up to (excluding) 10.0.17763.5329					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5487
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5489
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5490
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5491
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5492
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5493
Concurrent Execution using Shared Resource with Improper Synchronization	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5495
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5496
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5497
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5498
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5499
N/A	09-Jan-2024	6.5	Microsoft Message Queuing	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	date-guide/vulnerability/CVE-2024-20664	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5501
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5502
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5503
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5504
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5505
Exposure of Resource	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Disclosure Vulnerability **CVE ID : CVE-2024-20692**	lity/CVE-2024-20692	
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5507
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5508
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5509
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5510
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5511
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI)	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	guide/vulnerability/CVE-2024-21305	
Product: windows_10_21h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5513
Affected Version(s): * Up to (excluding) 10.0.19044.3930					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5514
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5515
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5516
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5518
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5519
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5520
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5521
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5522
Concurrent Execution using Shared Resource	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2024-21307**	lity/CVE-2024-21307	
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5524
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5525
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5526
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5527
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5529
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5530
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5531
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5532
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5533
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5535
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5536
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5537
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5538
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5539
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5541
Product: windows_10_22h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5542
Affected Version(s): * Up to (excluding) 10.0.19045.3930					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5543
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5544
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5545
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20683	guide/vulnerability/CVE-2024-20683	
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5547
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5548
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5549
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5550
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5552
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5553
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5554
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5555
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5556
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20664**	lity/CVE-2024-20664	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5558
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5559
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5560
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5561
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5562
Exposure of Resource	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Disclosure Vulnerability **CVE ID : CVE-2024-20692**	lity/CVE-2024-20692	
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5564
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5565
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5566
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5567
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5568
N/A	09-Jan-2024	4.7	Windows Themes Information	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20691**	guide/vulnerability/CVE-2024-20691	
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5570
Product: windows_11_21h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5571
Affected Version(s): * Up to (excluding) 10.0.22000.2713					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5572
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5573
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20682		
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5575
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5576
N/A	09-Jan-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21309	O-MIC-WIND-310124/5577
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5578
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5579
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5581
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5582
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5583
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5584
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5586
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5587
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5588
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5589
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5590
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5592
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5593
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5594
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5595
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5596
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21311		
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5598
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5599
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5600
Product: windows_11_22h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5601
Affected Version(s): * Up to (excluding) 10.0.22621.3007					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5602
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2024-20681**	guide/vulnerability/CVE-2024-20681	
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5604
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5605
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5606
N/A	09-Jan-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21309	O-MIC-WIND-310124/5607
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5608
Uncontrolled Resource	09-Jan-2024	7.5	Microsoft Message Queuing Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Service Vulnerability **CVE ID : CVE-2024-20661**	guide/vulnerability/CVE-2024-20661	
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5610
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5611
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5612
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5613
N/A	09-Jan-2024	7.3	Windows Libarchive Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2024-20697**	guide/vulnerability/CVE-2024-20697	
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5615
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5616
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5617
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5618
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5620
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5621
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5622
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5623
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5624
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5626
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5627
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5628
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5629
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5630
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21305		
Product: windows_11_23h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5632
Affected Version(s): * Up to (excluding) 10.0.22631.3007					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5633
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5634
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5635
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5636
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2024-20698**	guide/vulnerability/CVE-2024-20698	
N/A	09-Jan-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21309	O-MIC-WIND-310124/5638
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5639
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5640
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5641
Concurrent Execution using Shared Resource with Improper Synchronization	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5643
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5644
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20697	O-MIC-WIND-310124/5645
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5646
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5647
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC)	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure **CVE ID : CVE-2024-20663**	guide/vulnerability/CVE-2024-20663	
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5649
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5650
N/A	09-Jan-2024	6.5	Windows Nearby Sharing Spoofing Vulnerability **CVE ID : CVE-2024-20690**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20690	O-MIC-WIND-310124/5651
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5652
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5653
N/A	09-Jan-2024	6.1	Windows Server Key Distribution	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Security Feature Bypass **CVE ID : CVE-2024-21316**	lity/CVE-2024-21316	
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5655
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5656
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5657
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5658
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5660
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5661
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5662
Product: windows_server_2008					
Affected Version(s): -					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5663
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5664
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5666
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5667
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5668
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5669
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5670
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20692**	lity/CVE-2024-20692	
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5672
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5673
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5674
Affected Version(s): r2					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5676
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5677
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5678
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5679
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5680
Product: windows_server_2012					
Affected Version(s): -					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20674	lity/CVE-2024-20674	
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5682
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5683
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5684
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5685
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5686
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20660**	guide/vulnerability/CVE-2024-20660	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5688
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5689
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5690
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5691
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5692
Exposure of	09-Jan-2024	5.7	Microsoft Local Security Authority	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	date-guide/vulnerability/CVE-2024-20692	
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5694
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5695
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5696
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5697
Affected Version(s): r2					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20674	lity/CVE-2024-20674	
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5699
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5700
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5701
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5702
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5703
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20660**	guide/vulnerability/CVE-2024-20660	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5705
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5706
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5707
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5708
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5709
Exposure of	09-Jan-2024	5.7	Microsoft Local Security Authority	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	date-guide/vulnerability/CVE-2024-20692	
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5711
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5712
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5713
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5714
Product: windows_server_2016					
Affected Version(s): -					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20674	lity/CVE-2024-20674	
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5716
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5717
Uncontrolled Resource Consumption	09-Jan-2024	7.5	Microsoft Message Queuing Denial of Service Vulnerability **CVE ID : CVE-2024-20661**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20661	O-MIC-WIND-310124/5718
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5719
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5720
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5722
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5723
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20664**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20664	O-MIC-WIND-310124/5724
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5725
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5726
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20691	lity/CVE-2024-20691	
Affected Version(s): * Up to (excluding) 10.0.14393.6614					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5728
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5729
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5730
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5731
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20694		
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5733
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5734
Product: windows_server_2019					
Affected Version(s): -					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5735
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5736
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5737
Uncontrolled Resource	09-Jan-2024	7.5	Microsoft Message Queuing Denial of	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Service Vulnerability **CVE ID : CVE-2024-20661**	guide/vulnerability/CVE-2024-20661	
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5739
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5740
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5741
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5742
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5743
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20664**	lity/CVE-2024-20664	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5745
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5746
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5747
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5748
Affected Version(s): * Up to (excluding) 10.0.17763.5329					
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5749
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	date-guide/vulnerability/CVE-2024-21310	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5751
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5752
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5753
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5755
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5756
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5757
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5758
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5759
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21313		
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5761
Product: windows_server_2022					
Affected Version(s): -					
Authentication Bypass by Spoofing	09-Jan-2024	8.8	Windows Kerberos Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20674**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674	O-MIC-WIND-310124/5762
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5763
N/A	09-Jan-2024	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2024-20682**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20682	O-MIC-WIND-310124/5764
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20683**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20683	O-MIC-WIND-310124/5765
Uncontrolled	09-Jan-2024	7.5	Microsoft Message Queuing Denial of	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Service Vulnerability **CVE ID : CVE-2024-20661**	date-guide/vulnerability/CVE-2024-20661	
N/A	09-Jan-2024	7.5	Microsoft AllJoyn API Denial of Service Vulnerability **CVE ID : CVE-2024-20687**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20687	O-MIC-WIND-310124/5767
N/A	09-Jan-2024	7.5	.NET Framework Denial of Service Vulnerability **CVE ID : CVE-2024-21312**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312	O-MIC-WIND-310124/5768
N/A	09-Jan-2024	6.6	BitLocker Security Feature Bypass Vulnerability **CVE ID : CVE-2024-20666**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666	O-MIC-WIND-310124/5769
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-20660**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20660	O-MIC-WIND-310124/5770
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20663**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20663	O-MIC-WIND-310124/5771
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-20664**	lity/CVE-2024-20664	
N/A	09-Jan-2024	6.5	Windows Message Queuing Client (MSMQC) Information Disclosure **CVE ID : CVE-2024-20680**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20680	O-MIC-WIND-310124/5773
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2024-20699**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20699	O-MIC-WIND-310124/5774
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5775
N/A	09-Jan-2024	4.7	Windows Themes Information Disclosure Vulnerability **CVE ID : CVE-2024-20691**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20691	O-MIC-WIND-310124/5776
Affected Version(s): * Up to (excluding) 10.0.20348.2227					
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5777
Concurrent Execution	09-Jan-2024	7.5	Windows Hyper-V Remote Code	https://msrc.microsoft.com/up	O-MIC-WIND-310124/5778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2024-20700**	date-guide/vulnerability/CVE-2024-20700	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2024-21307**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21307	O-MIC-WIND-310124/5779
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20696**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20696	O-MIC-WIND-310124/5780
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5781
N/A	09-Jan-2024	6.5	Windows Themes Spoofing Vulnerability **CVE ID : CVE-2024-21320**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21320	O-MIC-WIND-310124/5782
N/A	09-Jan-2024	6.1	Windows Server Key Distribution	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Security Feature Bypass **CVE ID : CVE-2024-21316**	guide/vulnerability/CVE-2024-21316	
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5784
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5785
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5786
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information Disclosure Vulnerability **CVE ID : CVE-2024-21311**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21311	O-MIC-WIND-310124/5787
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5789
Affected Version(s): * Up to (excluding) 10.0.25398.643					
N/A	09-Jan-2024	7.8	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21309**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21309	O-MIC-WIND-310124/5790
Product: windows_server_2022_23h2					
Affected Version(s): -					
N/A	09-Jan-2024	7.8	Windows Subsystem for Linux Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20681**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20681	O-MIC-WIND-310124/5791
N/A	09-Jan-2024	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20686**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20686	O-MIC-WIND-310124/5792
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability **CVE ID : CVE-2024-20697**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20697	O-MIC-WIND-310124/5793
N/A	09-Jan-2024	5.5	Windows Hyper-V Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-310124/5794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20699	guide/vulnerability/CVE-2024-20699	
N/A	09-Jan-2024	4.9	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability **CVE ID : CVE-2024-20662**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20662	O-MIC-WIND-310124/5795
Affected Version(s): * Up to (excluding) 10.0.25398.643					
N/A	09-Jan-2024	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2024-20698**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20698	O-MIC-WIND-310124/5796
N/A	09-Jan-2024	7.8	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21310**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310	O-MIC-WIND-310124/5797
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Jan-2024	7.5	Windows Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2024-20700**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700	O-MIC-WIND-310124/5798
N/A	09-Jan-2024	7.3	Windows Libarchive Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20696	lity/CVE-2024-20696	
N/A	09-Jan-2024	6.5	Microsoft Message Queuing Information Disclosure Vulnerability **CVE ID : CVE-2024-21314**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21314	O-MIC-WIND-310124/5800
N/A	09-Jan-2024	6.1	Windows Server Key Distribution Service Security Feature Bypass **CVE ID : CVE-2024-21316**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21316	O-MIC-WIND-310124/5801
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.7	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability **CVE ID : CVE-2024-20692**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20692	O-MIC-WIND-310124/5802
N/A	09-Jan-2024	5.7	Microsoft Bluetooth Driver Spoofing Vulnerability **CVE ID : CVE-2024-21306**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21306	O-MIC-WIND-310124/5803
Exposure of Resource to Wrong Sphere	09-Jan-2024	5.5	Windows CoreMessaging Information Disclosure Vulnerability **CVE ID : CVE-2024-20694**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20694	O-MIC-WIND-310124/5804
N/A	09-Jan-2024	5.5	Windows Cryptographic Services Information	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-310124/5805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2024-21311**	lity/CVE-2024-21311	
N/A	09-Jan-2024	5.3	Windows TCP/IP Information Disclosure Vulnerability **CVE ID : CVE-2024-21313**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21313	O-MIC-WIND-310124/5806
N/A	09-Jan-2024	4.4	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability **CVE ID : CVE-2024-21305**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21305	O-MIC-WIND-310124/5807
Vendor: Qnap					
Product: qts					
Affected Version(s): 5.1.0.2348					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5809
Buffer Copy without	05-Jan-2024	7.2	A buffer copy without checking size of input	https://www.qnap.com/en/security-	O-QNA-QTS-310124/5810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**	advisory/qsa-23-27	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5812
Buffer Copy	05-Jan-2024	7.2	A buffer copy without checking	https://www.qnap.com/en/sec	O-QNA-QTS-310124/5813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	urity-advisory/qsa-23-27	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network.	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.1.0.2399					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5816
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5822
Buffer Copy without Checking Size of Input ('Classic	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): 5.1.0.2418					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5825
Buffer Copy without	05-Jan-2024	7.2	A buffer copy without checking size of input	https://www.qnap.com/en/security-	O-QNA-QTS-310124/5826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**	advisory/qsa-23-27	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5828
Buffer Copy	05-Jan-2024	7.2	A buffer copy without checking	https://www.qnap.com/en/sec	O-QNA-QTS-310124/5829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	urity-advisory/qsa-23-27	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network.	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.1.0.2444					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5832
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5835
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5838
Buffer Copy without	05-Jan-2024	7.2	A buffer copy without checking size of input	https://www.qnap.com/en/security-	O-QNA-QTS-310124/5839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	advisory/qsa-23-27	
Affected Version(s): 5.1.0.2466					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5847
Affected Version(s): 5.1.1.2491					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5855
Affected Version(s): 5.1.2.2533					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QTS-310124/5856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QTS-310124/5857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5859
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5863
Affected Version(s): 5.1.3.2578					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QTS-310124/5869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Product: quts_hero					
Affected Version(s): h5.1.0.2409					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20231110 and later **CVE ID : CVE-2023-39296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5871
Buffer Copy without Checking Size of Input ('Classic	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45041		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.0.2424					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39296		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5879
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.0.2453					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39296		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.0.2466					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39296		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5899
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.1.2488					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39296		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5907
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.2.2534					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Jan-2024	7.5	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	https://www.qnap.com/en/security-advisory/qsa-23-64	O-QNA-QUTS-310124/5910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39296		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Jan-2024	7.2	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later **CVE ID : CVE-2023-39294**	https://www.qnap.com/en/security-advisory/qsa-23-54	O-QNA-QUTS-310124/5911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45039**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5915
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**		
Affected Version(s): h5.1.3.2578					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45039		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45040**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45042**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45043**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.2	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later **CVE ID : CVE-2023-45044**	https://www.qnap.com/en/security-advisory/qsa-23-27	O-QNA-QUTS-310124/5923
Vendor: Qualcomm					
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5925
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5926
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5927
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5928
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-315_-310124/5929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5930
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5931
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-315_-310124/5932
Product: 9205_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9205-310124/5933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9205-310124/5934
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9205-310124/5935
Product: 9206_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9206-310124/5936
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9206-310124/5937
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9206-310124/5938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9206-310124/5939
Product: 9207_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9207-310124/5940
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-9207-310124/5941
Product: apq8017_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5943
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5944
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5945
Product: apq8037_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5946
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-APQ8-310124/5947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Product: apq8064au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5948
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5949
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5950
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: apq8076_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5952
Product: apq8084_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5953
Product: apq8092_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-APQ8-310124/5954
Product: apq8094_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-APQ8-310124/5955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: aqt1000_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5956
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5957
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5958
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-AQT1-310124/5959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5960
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5961
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5962
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5964
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5965
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5966
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AQT1-310124/5967
Product: ar8031_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-AR80-310124/5968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5969
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5970
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5971
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5973
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5974
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5975
Product: ar8035_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5976
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	O-QUA-AR80-310124/5977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5978
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5979
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5980
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5981
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-AR80-310124/5982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5983
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5984
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5986
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5987
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5988
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5989
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5991
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5992
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5993
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR80-310124/5994
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-AR80-310124/5995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: ar9380_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR93-310124/5996
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR93-310124/5997
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR93-310124/5998
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-AR93-310124/5999
Product: c-v2x_9150_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-C-V2-310124/6000
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-C-V2-310124/6001
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-C-V2-310124/6002
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-C-V2-310124/6003
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-C-V2-310124/6004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Product: csr8811_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSR8-310124/6005
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSR8-310124/6006
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSR8-310124/6007
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSR8-310124/6008
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	O-QUA-CSR8-310124/6009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSR8-310124/6010
Product: csra6620_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6011
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6012
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6014
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6015
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6016
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6017
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-CSRA-310124/6018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6019
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6020
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6021
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-CSRA-310124/6022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6023
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6024
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6025
Product: csra6640_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6027
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6028
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6029
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6030
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6032
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6033
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6034
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-CSRA-310124/6035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6036
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6037
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6038
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRA-310124/6039
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-CSRA-310124/6040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: csrb31024_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6041
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6042
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6043
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6044
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-CSRB-310124/6045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6046
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6047
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6048
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-CSRB-310124/6049
Product: fastconnect_6200_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6050
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6051
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6052
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6053
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6055
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6056
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6057
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6059
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6060
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6061
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6063
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6064
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6065
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6066
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6068
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6069
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6070
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6071
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-FAST-310124/6072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6073
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6074
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6075
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6076
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	O-QUA-FAST-310124/6077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6078
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6079
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6081
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6082
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6083
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6084
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6086
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6087
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6088
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6090
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6091
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6092
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6093
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-FAST-310124/6094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6095
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6096
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6097
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-FAST-310124/6098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6099
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6100
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6101
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6102
Product: fastconnect_6900_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6103
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6104
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6105
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6108
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6109
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6110
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6112
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6113
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6114
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6116
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6117
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6118
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6119
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6121
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6122
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6123
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6124
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6126
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6127
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6128
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6130
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6131
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6132
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6133
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-FAST-310124/6134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6135
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6136
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6137
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FAST-310124/6138
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-FAST-310124/6139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-FAST-310124/6140
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-FLIG-310124/6141
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-FLIG-310124/6142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-FLIG-310124/6143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6144
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6145
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6146
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6148
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6149
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6150
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6152
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6153
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6154
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FLIG-310124/6155
Product: fsm10056_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-FSM1-310124/6156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-FSM1-310124/6157
Product: home_hub_100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-HOME-310124/6158
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-HOME-310124/6159
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-HOME-310124/6160
Product: immersive_home_214_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6161
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6162
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6163
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6164
Product: immersive_home_216_platform_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IMME-310124/6165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6166
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6167
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6168
Product: immersive_home_316_platform_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6169
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-IMME-310124/6170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IMME-310124/6171
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IMME-310124/6172
Product: immersive_home_318_platform_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IMME-310124/6173
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IMME-310124/6174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6175
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6176
Product: immersive_home_3210_platform_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6177
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6178
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IMME-310124/6179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6180
Product: immersive_home_326_platform_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6181
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6182
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IMME-310124/6183
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-IMME-310124/6184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: ipq4018_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6185
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6186
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6187
Product: ipq4019_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/produc	O-QUA-IPQ4-310124/6188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	t-security/bulletins/january-2024-bulletin	
Product: ipq4028_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6189
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6190
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6191
Product: ipq4029_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ4-310124/6192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6193
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ4-310124/6194
Product: ipq5010_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6195
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6196
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	O-QUA-IPQ5-310124/6197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6198
Product: ipq5028_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6199
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6200
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6202
Product: ipq5332_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6203
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ5-310124/6204
Product: ipq6000_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ6-310124/6205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6206
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6207
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6208
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6209
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: ipq6005_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6211
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6212
Product: ipq6010_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6213
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6214
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	O-QUA-IPQ6-310124/6215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6216
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6217
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6218
Product: ipq6018_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6220
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6221
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6222
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6223
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq6028_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6225
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6226
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6227
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6228
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ6-310124/6230
Product: ipq8064_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6231
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6232
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6233
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-310124/6234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: ipq8065_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6235
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6236
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6237
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8068_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6239
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6240
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6241
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6242
Product: ipq8069_firmware					
Affected Version(s): -					
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-IPQ8-310124/6243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6244
Product: ipq8070a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6245
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6246
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6248
Product: ipq8070_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6249
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6250
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6251
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-310124/6252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: ipq8071a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6253
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6254
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6255
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8072a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6257
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6258
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6259
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6260
Product: ipq8074a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-IPQ8-310124/6261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6262
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6263
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6264
Product: ipq8074_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6266
Product: ipq8076a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6267
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6268
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6269
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-310124/6270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: ipq8076_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6271
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6272
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6273
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8078a_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6275
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6276
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6277
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6278
Product: ipq8078_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-IPQ8-310124/6279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6280
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6281
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6282
Product: ipq8173_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6284
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6285
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6286
Product: ipq8174_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6287
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-310124/6288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6289
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ8-310124/6290
Product: ipq9008_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6291
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6292
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-IPQ9-310124/6293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IPQ9-310124/6294
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IPQ9-310124/6295
Product: ipq9554_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IPQ9-310124/6296
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-IPQ9-310124/6297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6298
Product: ipq9570_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6299
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6300
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6301
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ9-310124/6302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: ipq9574_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6303
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6304
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6305
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-IPQ9-310124/6306
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-IPQ9-310124/6307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: mdm8207_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM8-310124/6308
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM8-310124/6309
Product: mdm9225m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6310
Product: mdm9225_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-MDM9-310124/6311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Product: mdm9230_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6312
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6313
Product: mdm9235m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6314
Product: mdm9250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-310124/6315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6316
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6317
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6318
Product: mdm9330_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6320
Product: mdm9625m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6321
Product: mdm9625_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6322
Product: mdm9628_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6324
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6325
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6326
Product: mdm9630_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6327
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	O-QUA-MDM9-310124/6328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
Product: mdm9635m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6329
Product: mdm9640_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6330
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6331
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6333
Product: mdm9645_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6334
Product: mdm9650_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6335
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-310124/6336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6337
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6338
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6339
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MDM9-310124/6340
Product: msm8108_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6341
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6342
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6343
Product: msm8209_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6344
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6346
Product: msm8608_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6347
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6348
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6349
Product: msm8909w_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6350
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6351
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6352
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6353
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6355
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-MSM8-310124/6356
Product: pm8937_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-PM89-310124/6357
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-PM89-310124/6358
Product: pmp8074_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-PMP8-310124/6359
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-PMP8-310124/6360
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-PMP8-310124/6361
Product: qam8255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6362
Buffer Copy without Checking Size of Input	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QAM8-310124/6363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6364
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6365
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6366
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6368
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6369
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6370
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6372
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6373
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6374
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6375
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QAM8-310124/6376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: qam8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6377
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6378
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6379
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6380
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a	https://www.qualcomm.com/company/product-	O-QUA-QAM8-310124/6381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6382
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6383
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6385
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6386
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6387
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6388
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-QAM8-310124/6389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6390
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6391
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6392
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qam8650p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6394
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6395
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6396
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6397
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QAM8-310124/6398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6399
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6400
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6401
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	O-QUA-QAM8-310124/6402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6403
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6404
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6405
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6407
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6408
Product: qam8775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6409
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6410
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QAM8-310124/6411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6412
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6413
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6414
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6416
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6417
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6418
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6419
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	O-QUA-QAM8-310124/6420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6421
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6422
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QAM8-310124/6423
Product: qca0000_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA0-310124/6424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA0-310124/6425
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA0-310124/6426
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA0-310124/6427
Product: qca1023_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qca1062_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6429
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6430
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6431
Product: qca1064_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6433
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6434
Product: qca1990_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA1-310124/6435
Product: qca2062_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA2-310124/6436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6437
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6438
Product: qca2064_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6439
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6440
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-QCA2-310124/6441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qca2065_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6442
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6443
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6444
Product: qca2066_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/c	O-QUA-QCA2-310124/6445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6446
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA2-310124/6447
Product: qca4004_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6448
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6450
Product: qca4024_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6451
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6452
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6453
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6455
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6456
Product: qca4531_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA4-310124/6457
Product: qca6174a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6459
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6460
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6461
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6462
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6464
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6465
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6466
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6468
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6469
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6470
Product: qca6174_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6471
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6473
Product: qca6175a_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6474
Product: qca6234_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6475
Product: qca6310_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6476
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6477
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6478
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6479
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6480
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-QCA6-310124/6481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6482
Product: qca6320_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6483
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6484
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6486
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6487
Product: qca6335_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6488
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6489
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6491
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6492
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6493
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6494
Product: qca6391_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6495
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6496
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6497
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6500
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6501
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6502
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6504
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6505
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6506
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6508
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6509
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6510
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6511
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6512
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-QCA6-310124/6513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6514
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6515
Product: qca6420_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6517
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6518
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6519
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6520
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6522
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6523
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6524
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6525
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6527
Product: qca6421_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6528
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6529
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6530
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOA	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6532
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6533
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6534
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6536
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6537
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6538
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6426_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6540
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6541
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6542
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6543
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6545
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6546
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6547
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6549
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6550
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6551
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6552
Product: qca6428_firmware					
Affected Version(s): -					
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-QCA6-310124/6553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6554
Product: qca6430_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6555
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6556
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.q ualcomm.com/c ompany/produc t-security/bulleti	O-QUA-QCA6-310124/6557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6558
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6559
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6560
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6562
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6563
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6564
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6565
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036	ns/january-2024-bulletin	
Product: qca6431_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6567
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6568
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6569
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6571
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6572
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6573
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6574
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6576
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6577
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6578
Product: qca6436_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6580
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6581
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6582
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6583
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6585
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6586
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6587
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6588
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-QCA6-310124/6589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6590
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6591
Product: qca6438_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6592
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qca6554a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6594
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6595
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6596
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6598
Product: qca6564au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6599
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6600
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6601
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6603
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6604
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6605
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6606
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6608
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6609
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6610
Product: qca6564a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6612
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6613
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6614
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6615
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			support makes a PSCI call. **CVE ID : CVE-2023-33036**	ns/january-2024-bulletin	
Product: qca6564_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6617
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6618
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6619
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6620
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-QCA6-310124/6621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: qca6574au_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6622
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6623
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6624
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6626
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6627
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6628
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6630
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6631
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6632
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6634
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6635
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6636
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6637
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-QCA6-310124/6638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6639
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6640
NULL Pointer Dereferenc e	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6641
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA6-310124/6642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6574a_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6643
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6644
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6645
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6646
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6648
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6649
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6650
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6652
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6653
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6654
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6656
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6657
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6658
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6659
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6661
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6662
Product: qca6574_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6663
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6664
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6666
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6667
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6668
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6670
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6671
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6672
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6674
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6675
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6676
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6677
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-QCA6-310124/6678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6679
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6680
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6681
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6683
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6684
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6685
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6686
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6688
Product: qca6584_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6689
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6690
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6692
Product: qca6595au_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6693
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6694
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6695
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6697
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6698
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6699
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6701
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6702
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6703
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6705
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6706
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6707
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6708
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6710
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6711
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6712
Product: qca6595_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6714
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6715
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6716
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6717
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_CO	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6719
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6720
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6721
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	O-QUA-QCA6-310124/6722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6723
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6724
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6725
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6727
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6728
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6729
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6678aq_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6731
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6732
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6733
Product: qca6696_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6735
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6736
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6737
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6738
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6740
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6741
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6742
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6744
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6745
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6746
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6748
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6749
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6750
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6751
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6753
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6754
Product: qca6698aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6755
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6756
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6758
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6759
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6760
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6762
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6763
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6764
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6766
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6767
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6768
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6769
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	O-QUA-QCA6-310124/6770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6771
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6772
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6773
Product: qca6797aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-310124/6774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6775
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6776
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6777
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6778
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-QCA6-310124/6779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6780
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6781
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6783
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6784
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6785
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6786
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA6-310124/6788
Product: qca7500_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA7-310124/6789
Product: qca8072_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6790
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6791
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-QCA8-310124/6792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6793
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6794
Product: qca8075_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6795
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6797
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6798
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6799
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6800
Product: qca8081_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-310124/6801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33025**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6802
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6803
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6804
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6805
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6807
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6808
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6809
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6811
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6812
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6813
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6814
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-310124/6815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6816
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6817
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6818
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6819
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in Automotive while	https://www.qualcomm.com/company/produc	O-QUA-QCA8-310124/6820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	t-security/bulletins/january-2024-bulletin	
Product: qca8082_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6821
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6822
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6823
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6824
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-QCA8-310124/6825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: qca8084_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6826
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6827
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6828
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6830
Product: qca8085_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6831
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6832
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6834
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6835
Product: qca8337_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6836
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6837
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-310124/6838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6840
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6841
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6842
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-310124/6843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6844
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6845
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6847
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6848
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6849
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6850
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6852
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6853
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6854
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6855
Product: qca8386_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6856
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6857
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6858
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6859
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA8-310124/6860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9367_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6861
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6862
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6863
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6864
Product: qca9377_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6865
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6866
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6867
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6870
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6871
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6872
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6874
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6875
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6876
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6877
Product: qca9379_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6878
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6879
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6880
Product: qca9880_firmware					
Affected Version(s): -					
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6881
Product: qca9886_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	O-QUA-QCA9-310124/6882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6883
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6884
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6885
Product: qca9888_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6886
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-QCA9-310124/6887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_ mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA9-310124/6888
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA9-310124/6889
Product: qca9889_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA9-310124/6890
NULL Pointer Dereferenc e	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-QCA9-310124/6891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6892
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6893
Product: qca9898_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6894
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6895
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA9-310124/6896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qca9980_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6897
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6898
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6899
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9984_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6901
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6902
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6903
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6904
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6905
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-QCA9-310124/6906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qca9985_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6907
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6908
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6909
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qca9986_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6911
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6912
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6913
Product: qca9990_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6915
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6916
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6917
Product: qca9992_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6918
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA9-310124/6919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6920
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6921
Product: qca9994_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6922
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6923
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	O-QUA-QCA9-310124/6924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCA9-310124/6925
Product: qcc2073_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6926
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6927
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcc2076_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6929
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6930
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC2-310124/6931
Product: qcc710_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6933
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6934
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6935
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCC7-310124/6936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6937
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCC7-310124/6938
Product: qcf8001_firmware					
Affected Version(s): -					
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCF8-310124/6939
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCF8-310124/6940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCF8-310124/6941
Product: qcm2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6942
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6943
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6944
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM2-310124/6945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6946
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6947
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6948
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM2-310124/6949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6950
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM2-310124/6951
Product: qcm4290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6952
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6953
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-QCM4-310124/6954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6955
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6956
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6957
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-QCM4-310124/6958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6959
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6960
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6961
Product: qcm4325_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6964
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6965
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6966
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6968
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6969
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6970
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM4-310124/6971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6972
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6973
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6974
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6975
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM4-310124/6976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: qcm4490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6977
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6978
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6979
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6980
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	O-QUA-QCM4-310124/6981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6982
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6983
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6984
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6985
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM4-310124/6986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM4-310124/6987
Product: qcm6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6988
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6989
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6991
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6992
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6993
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6994
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-QCM6-310124/6995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6996
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6997
Product: qcm6490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6998
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/6999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7000
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7001
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7002
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7003
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7005
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7006
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7007
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM6-310124/7008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7009
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7010
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7011
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM6-310124/7012
Product: qcm8550_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK	https://www.qualcomm.com/company/produc	O-QUA-QCM8-310124/7013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7014
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7015
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7016
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-QCM8-310124/7017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7018
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7019
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7020
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCM8-310124/7022
Product: qcn5021_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7023
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7024
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7025
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN5-310124/7026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7027
Product: qcn5022_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7028
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7029
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7030
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-QCN5-310124/7031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7032
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7033
Product: qcn5024_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7034
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7036
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7037
Product: qcn5052_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7038
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7039
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN5-310124/7040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7041
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7042
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7043
Product: qcn5054_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7044
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-QCN5-310124/7045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7046
Product: qcn5121_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7047
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7048
Product: qcn5122_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN5-310124/7049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7050
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7051
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7052
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7053
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn5124_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7055
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7056
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7057
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7058
Product: qcn5152_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7059
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7060
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7061
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7062
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7063
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-QCN5-310124/7064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qcn5154_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7065
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7066
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7067
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn5164_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7069
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7070
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7071
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN5-310124/7072
Product: qcn6023_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7073
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7074
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7075
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7076
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7077
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-QCN6-310124/7078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qcn6024_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7079
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7080
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7081
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7083
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7084
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7085
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7086
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7088
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7089
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7090
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7091
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7093
Product: qcn6100_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7094
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7095
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7096
Product: qcn6102_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7097
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7098
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7099
Product: qcn6112_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7100
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN6-310124/7101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7102
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7103
Product: qcn6122_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7104
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7105
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	O-QUA-QCN6-310124/7106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7107
Product: qcn6132_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7108
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7109
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7111
Product: qcn6224_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7112
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7113
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	O-QUA-QCN6-310124/7114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7115
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7116
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7117
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn6274_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7119
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7120
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7121
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	O-QUA-QCN6-310124/7122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7123
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7124
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN6-310124/7125
Product: qcn7605_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN7-310124/7126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7127
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7128
Product: qcn7606_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7129
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7130
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-QCN7-310124/7131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7132
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing GATT service data when the total amount of memory that is required by the multiple services is greater than the actual size of the services buffer. **CVE ID : CVE-2023-43512**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN7-310124/7133
Product: qcn9000_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7134
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	O-QUA-QCN9-310124/7135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7136
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7137
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7138
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7139
Product: qcn9001_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7140
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7141
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7142
Product: qcn9002_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7143
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN9-310124/7144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7145
Product: qcn9003_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7146
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7147
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9011_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7149
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7151
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7152
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7154
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7155
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7156
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-QCN9-310124/7157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7158
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7159
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7160
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7161
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-QCN9-310124/7162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: qcn9012_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7163
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7165
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7167
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7168
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7169
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7171
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7172
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7173
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7174
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_	https://www.qualcomm.com/company/product-	O-QUA-QCN9-310124/7175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7176
Product: qcn9013_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7177
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7178
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7180
Product: qcn9022_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7181
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7182
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7183
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN9-310124/7184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7185
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7186
Product: qcn9024_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7187
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7188
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while	https://www.qualcomm.com/company/produc	O-QUA-QCN9-310124/7189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7190
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7192
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7193
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	O-QUA-QCN9-310124/7194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7195
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7196
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7197
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7198
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN9-310124/7199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33116	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7200
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7201
Product: qcn9070_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7202
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7204
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7205
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7206
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7207
Product: qcn9072_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN9-310124/7208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7209
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7210
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7211
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7212
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Product: qcn9074_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7214
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7215
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7216
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7217
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN9-310124/7218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7219
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7220
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7221
Product: qcn9100_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7222
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-QCN9-310124/7223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7224
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7225
Product: qcn9274_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7226
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7228
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7229
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCN9-310124/7230
Product: qcs2290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7231
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS2-310124/7232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7233
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7234
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7235
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7237
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7238
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7239
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS2-310124/7240
Product: qcs410_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7241
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7242
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7243
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7244
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7245
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-QCS4-310124/7246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7247
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7248
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7250
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7251
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7252
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7253
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS4-310124/7254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7255
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7256
Product: qcs4290_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7257
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7258
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-QCS4-310124/7259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7260
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7261
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7262
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-QCS4-310124/7263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7264
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7265
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7266
Product: qcs4490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7268
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7269
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7270
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7271
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7272
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-QCS4-310124/7273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7274
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7275
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7276
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS4-310124/7277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs610_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7278
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7279
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7280
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7283
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7284
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7285
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7287
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7288
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7289
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7290
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-QCS6-310124/7291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7292
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7293
Product: qcs6125_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7294
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7296
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7297
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7298
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7299
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-QCS6-310124/7300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7301
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7302
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7303
Product: qcs6490_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7305
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7306
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7307
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7308
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7310
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7311
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7312
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS6-310124/7313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7314
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7315
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7316
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7317
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	O-QUA-QCS6-310124/7318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS6-310124/7319
Product: qcs7230_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7320
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7321
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS7-310124/7322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7323
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7324
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7325
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	O-QUA-QCS7-310124/7326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7327
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7328
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7329
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS7-310124/7330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8155_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7331
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7332
Product: qcs8250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7333
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7334
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7336
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7337
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7338
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7340
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7341
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7342
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS8-310124/7343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7344
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7345
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7346
Product: qcs8550_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7348
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7349
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7350
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7351
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7353
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7354
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7355
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7357
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7358
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7359
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7360
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7362
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QCS8-310124/7363
Product: qdu1000_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7364
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7366
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7367
Product: qdu1010_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7368
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7369
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	O-QUA-QDU1-310124/7370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7371
Product: qdu1110_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7372
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7373
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QDU1-310124/7374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7375
Product: qdu1210_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7376
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7377
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDU1-310124/7379
Product: qdx1010_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7380
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7381
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7383
Product: qdx1011_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7384
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7385
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QDX1-310124/7386
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives	https://www.qualcomm.com/company/produc	O-QUA-QDX1-310124/7387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	t-security/bulletins/january-2024-bulletin	
Product: qet4101_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QET4-310124/7388
Product: qfw7114_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7389
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7391
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7392
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7393
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7394
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QFW7-310124/7395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qfw7124_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7396
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7397
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7399
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7400
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7401
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QFW7-310124/7402
Product: qrb5165m_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7403
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7404
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7405
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7406
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7408
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7409
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7410
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QRB5-310124/7411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7412
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7413
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7414
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7415
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QRB5-310124/7416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: qrb5165n_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7417
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7418
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7419
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7421
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7422
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7423
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7425
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7426
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7427
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7428
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	O-QUA-QRB5-310124/7429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7430
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRB5-310124/7431
Product: qru1032_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7432
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QRU1-310124/7433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7434
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7435
Product: qru1052_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7436
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7438
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7439
Product: qru1062_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7440
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7442
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QRU1-310124/7443
Product: qsm8250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7444
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7445
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7447
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7448
Product: qsm8350_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7449
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7450
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QSM8-310124/7451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7452
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7453
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSM8-310124/7454
Product: qsw8573_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QSW8-310124/7455
Product: qts110_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QTS1-310124/7456
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QTS1-310124/7457
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QTS1-310124/7458
Product: qualcomm_205_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7459
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7461
Product: qualcomm_215_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7462
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7463
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7464
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7466
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7467
Product: qualcomm_video_collaboration_vc1_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7468
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK	https://www.qualcomm.com/company/produc	O-QUA-QUAL-310124/7469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7470
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7471
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7472
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-QUAL-310124/7473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7474
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7475
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7476
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QUAL-310124/7477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7478
Product: qualcomm_video_collaboration_vc3_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7479
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7480
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7482
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7483
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7484
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QUAL-310124/7485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7486
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7487
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7488
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7489
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-QUAL-310124/7490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Product: qualcomm_video_collaboration_vc5_platform_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7491
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7492
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7493
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOA	https://www.qualcomm.com/company/product-	O-QUA-QUAL-310124/7494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7495
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7496
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7498
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7499
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7500
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-QUAL-310124/7501
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QUAL-310124/7502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: robotics_rb3_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7503
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7504
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7505
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7506
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-ROBO-310124/7507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7508
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7509
Product: robotics_rb5_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7510
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7512
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7513
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7514
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7515
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-ROBO-310124/7516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7517
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7518
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7520
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7521
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7522
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7523
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-ROBO-310124/7524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7525
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7526
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7528
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7530
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7531
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7532
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7534
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7535
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7536
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7537
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-SA41-310124/7538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7539
Product: sa4155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7540
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7541
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7543
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7544
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7545
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7546
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-SA41-310124/7547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7548
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7549
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7550
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	O-QUA-SA41-310124/7551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7552
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA41-310124/7553
Product: sa6145p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7555
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7556
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7557
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7559
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-SA61-310124/7560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7561
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7562
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7564
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7565
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7566
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7567
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA61-310124/7568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7569
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7570
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7571
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7572
Product: sa6150p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7573
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7574
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7575
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7576
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7578
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7579
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7580
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7581
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-SA61-310124/7582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7583
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7584
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7585
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-SA61-310124/7586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7587
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7588
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7589
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6155p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7591
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7592
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7593
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7594
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA61-310124/7595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7596
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7597
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7598
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7599
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	O-QUA-SA61-310124/7600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7601
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7602
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7604
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7605
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7606
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7607
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7609
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7610
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7611
Product: sa6155_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7613
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7614
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7615
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7616
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7618
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7619
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7620
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA61-310124/7621
Product: sa8145p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7623
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7624
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7625
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7626
Buffer Copy without Checking Size of	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7628
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7629
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7630
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7632
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7633
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7634
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7636
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7637
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7638
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7639
Product: sa8150p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer	https://www.qualcomm.com/company/produc	O-QUA-SA81-310124/7640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7641
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7642
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7643
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7644
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	O-QUA-SA81-310124/7645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7646
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7647
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7648
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7650
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7651
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7652
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7654
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7655
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7656
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7657
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the	https://www.qualcomm.com/company/product-	O-QUA-SA81-310124/7658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	security/bulletins/january-2024-bulletin	
Product: sa8155p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7659
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7660
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7661
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7663
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7664
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7665
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7666
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7668
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7669
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7671
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7672
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7673
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7674
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7676
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7677
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7678
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7679
Product: sa8155_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7680
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7681
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7682
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7683
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7685
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7686
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7687
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7688
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa8195p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7690
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7691
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7692
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7693
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-310124/7694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7695
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7696
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7697
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7698
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when	https://www.qualcomm.com/company/produc	O-QUA-SA81-310124/7699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7700
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7701
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7703
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7704
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7705
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7706
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7708
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA81-310124/7709
Product: sa8255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7712
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7713
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7714
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7715
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-SA82-310124/7716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7717
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7718
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7719
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA82-310124/7720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7721
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7722
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7723
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7725
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7726
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7727
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7728
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33108		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7730
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7731
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7732
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA82-310124/7733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7734
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7735
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7736
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7738
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7739
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7740
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA82-310124/7741
Product: sa8540p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA85-310124/7742
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA85-310124/7743
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA85-310124/7744
Product: sa9000p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA90-310124/7745
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA90-310124/7746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SA90-310124/7747
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7748
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7749
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7750
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7752
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7753
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7754
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SC81-310124/7755
Product: sd460_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	O-QUA-SD46-310124/7756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7757
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7758
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7759
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7760
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD46-310124/7762
Product: sd626_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD62-310124/7763
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD62-310124/7764
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD62-310124/7765
Product: sd660_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7766
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7767
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7768
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7769
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD66-310124/7770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7771
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7772
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7773
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7775
Product: sd662_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7776
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7777
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7778
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/product-	O-QUA-SD66-310124/7779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7780
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7781
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD66-310124/7782
Product: sd670_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7784
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7785
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7786
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7787
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7789
Product: sd675_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7790
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7791
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7792
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD67-310124/7793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7794
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7795
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7796
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7797
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD67-310124/7799
Product: sd730_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7800
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7801
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7802
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-SD73-310124/7803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7804
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7805
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7806
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7808
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD73-310124/7809
Product: sd820_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD82-310124/7810
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD82-310124/7811
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD82-310124/7812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: sd821_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD82-310124/7813
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD82-310124/7814
Product: sd835_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD83-310124/7815
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD83-310124/7816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD83-310124/7817
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD83-310124/7818
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD83-310124/7819
Product: sd855_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gets an IPv6 address. **CVE ID : CVE-2023-28583**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7821
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7822
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7823
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7824
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7826
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7827
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7828
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7829
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-SD85-310124/7830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD85-310124/7831
Product: sd865_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7832
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7833
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7835
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7836
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7837
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7839
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7840
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7841
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7842
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD86-310124/7843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7844
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD86-310124/7845
Product: sd888_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7846
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7848
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7849
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7850
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7851
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7853
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7854
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7855
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7857
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7858
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD88-310124/7859
Product: sdm429w_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDM4-310124/7860
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDM4-310124/7861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDM4-310124/7862
Product: sdx20m_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX2-310124/7863
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX2-310124/7864
Product: sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS	https://www.qualcomm.com/company/produc	O-QUA-SDX5-310124/7865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while running playready use-case. **CVE ID : CVE-2023-33030**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7866
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7867
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7869
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDX5-310124/7870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7871
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7872
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7873
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7875
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7876
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7877
Product: sdx57m_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7878
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDX5-310124/7879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7880
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7881
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX5-310124/7882
Product: sdx65m_firmware					
Affected Version(s): -					
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX6-310124/7883
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX6-310124/7884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX6-310124/7885
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SDX6-310124/7886
Product: sd_455_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_4-310124/7887
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_4-310124/7888
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD_4-310124/7889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: sd_675_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7890
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7891
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7892
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7893
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	O-QUA-SD_6-310124/7894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7895
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7896
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7897
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_6-310124/7899
Product: sd_8cx_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7900
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7901
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7902
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7904
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7905
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7906
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7907
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-	O-QUA-SD_8-310124/7908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7909
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7910
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7911
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SD_8-310124/7912
Missing Encryption	02-Jan-2024	5.5	Cryptographic issue in Automotive while	https://www.qualcomm.com/company/produc	O-QUA-SD_8-310124/7913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	t-security/bulletins/january-2024-bulletin	
Product: sg4150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7914
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7915
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7916
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7917
Use After Free	02-Jan-2024	7.8	Memory corruption when	https://www.qualcomm.com/c	O-QUA-SG41-310124/7918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7919
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7920
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43514		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7922
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7923
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7924
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG41-310124/7925
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SG41-310124/7926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: sg8275p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7927
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7928
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7929
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7931
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7932
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7933
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SG82-310124/7934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SG82-310124/7935
Product: sm4125_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7936
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7937
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7939
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7940
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7941
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-SM41-310124/7942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7943
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM41-310124/7944
Product: sm4450_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7945
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7947
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7948
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7949
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM44-310124/7950
Product: sm6250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7952
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7953
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7954
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7955
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7956
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SM62-310124/7957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7958
Product: sm6250_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7959
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7960
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7962
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7963
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7964
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7965
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-SM62-310124/7966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7967
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM62-310124/7968
Product: sm7250p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7969
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7971
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7972
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7973
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7975
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7976
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7977
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7978
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM72-310124/7979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7980
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7981
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM72-310124/7982
Product: sm7315_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7984
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7986
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7987
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7989
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7990
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7991
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7993
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7994
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7995
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7996
Product: sm7325p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM73-310124/7997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7998
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/7999
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8000
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8001
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8003
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8004
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8005
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM73-310124/8006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8007
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8008
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8009
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM73-310124/8010
Product: sm8550p_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK	https://www.qualcomm.com/company/produc	O-QUA-SM85-310124/8011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8012
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8013
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8014
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-SM85-310124/8015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8016
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8017
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8018
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SM85-310124/8020
Product: smart_audio_200_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8021
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8022
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8023
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-SMAR-310124/8024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Product: smart_audio_400_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8025
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8026
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8027
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8029
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8030
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8031
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8033
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8034
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8035
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8036
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SMAR-310124/8037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8038
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8039
Product: smart_display_200_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8040
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SMAR-310124/8042
Product: snapdragon_1100_wearable_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8043
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8044
Product: snapdragon_1200_wearable_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8045
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8047
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8048
Product: snapdragon_208_processor_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8049
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8051
Product: snapdragon_210_processor_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8052
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8053
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8054
Product: snapdragon_212_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8055
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8056
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8057
Product: snapdragon_425_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8058
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8060
Product: snapdragon_427_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8061
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8062
Concurrent Execution using Shared Resource with Improper Synchroniz	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_429_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8064
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8065
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8066
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_430_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8068
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8069
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_435_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8071
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8072
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8073
Product: snapdragon_439_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8074
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8075
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8076
Product: snapdragon_450_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8078
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8079
Product: snapdragon_460_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8080
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8082
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8083
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8084
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8086
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8087
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8088
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8089
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8091
Product: snapdragon_480\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8092
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8095
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8096
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8097
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8099
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8100
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8101
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8103
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8104
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8105
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8106
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_480_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8108
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8109
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8110
Buffer Copy without Checking	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8112
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8113
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8114
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8116
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8117
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8118
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8119
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8121
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8122
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Product: snapdragon_4_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8124
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8125
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8127
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8129
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8130
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8131
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8133
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8134
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8135
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8136
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8138
Product: snapdragon_4_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8139
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8140
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8142
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8143
Product: snapdragon_625_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8144
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8145
Concurrent Execution using Shared	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	security/bulletins/january-2024-bulletin	
Product: snapdragon_626_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8147
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8148
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_630_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8150
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8151
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8152
Concurrent Execution using Shared Resource with Improper Synchroniz	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_632_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8154
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8155
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_636_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8157
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8158
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8159
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_660_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8161
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8162
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8163
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8165
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8166
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8167
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8169
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8170
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_662_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8172
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8173
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8174
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8175
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8177
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8178
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8179
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8181
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8182
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8183
Product: snapdragon_665_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8184
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8185
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8186
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8187
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8189
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8190
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8191
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8192
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8194
Product: snapdragon_670_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8195
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8196
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8198
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8199
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8200
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8202
Product: snapdragon_675_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8203
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8204
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8206
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8207
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8208
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8210
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8211
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8212
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8214
Product: snapdragon_678_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8215
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8216
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8217
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8219
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8220
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8221
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8222
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8224
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8225
NULL Pointer Dereferenc e	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Product: snapdragon_680_4g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8227
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8228
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8229
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8230
Buffer Copy without Checking Size of Input	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8232
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8233
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8234
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8236
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8237
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8238
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8240
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8241
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8242
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8243
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8245
Product: snapdragon_685_4g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8246
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8248
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8250
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8251
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8253
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8254
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8255
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8257
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8258
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8259
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8260
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8262
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8263
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33037		
Product: snapdragon_690_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8265
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8266
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8267
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8268
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8270
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8271
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8273
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8274
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8275
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8276
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_695_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8278
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8279
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8280
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8282
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8283
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8284
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8286
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8287
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8288
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8289
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8291
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8292
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_710_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8294
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8295
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8296
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8297
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8299
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8300
Product: snapdragon_712_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8301
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8303
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8304
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8305
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_720g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8307
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8308
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8309
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8310
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-SNAP-310124/8311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8312
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8313
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8314
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8316
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8317
Product: snapdragon_730g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8319
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8320
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8321
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8322
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8324
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8325
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8326
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8327
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_730_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8329
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8330
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8332
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8333
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8334
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8335
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8337
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8338
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_732g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8340
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8341
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8342
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8343
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8345
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8346
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8347
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8348
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8350
Product: snapdragon_750g_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8351
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8353
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8354
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8355
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8357
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8358
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8359
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8360
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8362
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8363
Product: snapdragon_765g_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8365
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8366
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8367
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8368
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8370
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8371
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8372
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8374
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8375
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8376
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8378
Product: snapdragon_765_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8379
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8380
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8381
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.q ualcomm.com/c	O-QUA-SNAP-310124/8382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8383
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8384
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8386
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8387
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8388
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8389
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8391
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8392
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8393
Product: snapdragon_768g_5g_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8394
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8395
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8396
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8397
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8399
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8400
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8401
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8403
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8404
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8405
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8407
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8408
Product: snapdragon_778g\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8409
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8410
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8412
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8413
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8414
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8416
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8417
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8418
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8419
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8421
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8422
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_778g_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8424
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8425
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8427
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8429
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8430
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8431
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8433
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8434
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8435
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8436
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8438
Product: snapdragon_780g_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8439
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8440
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8442
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8443
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8444
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8446
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8447
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8448
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8449
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8451
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8452
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_782g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8454
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8455
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8456
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8457
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8459
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8460
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8461
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8463
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8464
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8465
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8466
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8468
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8469
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8470
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8472
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8473
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8474
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8476
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8477
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8478
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8479
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8481
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8482
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_7c_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8484
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8485
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8486
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8487
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8489
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8490
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8491
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Product: snapdragon_7c_gen_2_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8493
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8494
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8495
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8496
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8498
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8499
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8500
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_808_processor_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8502
Product: snapdragon_810_processor_firmware					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8503
Product: snapdragon_820_automotive_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8505
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8506
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8507
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8508
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8510
Product: snapdragon_820_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8511
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8512
Loop with Unreachable Exit	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	t-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8514
Product: snapdragon_821_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8515
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8517
Product: snapdragon_835_mobile_pc_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8518
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8519
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8521
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8522
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Product: snapdragon_845_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8524
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8525
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8526
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8527
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8529
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8530
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8531
Product: snapdragon_850_mobile_compute_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8532
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8533
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8534
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8535
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8537
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8538
Product: snapdragon_855\+\/860_mobile_platform_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8540
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8541
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8542
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8543
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8545
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8546
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8547
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8548
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8550
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8551
Product: snapdragon_855_mobile_platform_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8553
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8554
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8555
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8556
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8558
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8559
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8560
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8561
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8563
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8564
Product: snapdragon_865\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8566
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8567
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8568
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8569
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8571
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8572
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8573
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8575
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8576
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8577
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8579
Product: snapdragon_865_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8580
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8581
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8582
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.q ualcomm.com/c	O-QUA-SNAP-310124/8583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8584
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8585
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8587
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8588
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8589
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8590
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8592
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8593
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8594
Product: snapdragon_870_5g_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8595
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8596
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8597
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8598
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8600
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8601
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8602
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8604
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8605
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8606
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8608
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8609
Product: snapdragon_888\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8610
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8611
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	t-security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8613
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8614
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8615
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8617
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8618
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8619
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8620
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8622
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8623
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8625
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8626
Product: snapdragon_888_5g_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8627
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8628
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8630
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8631
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8632
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8634
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8635
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8636
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8637
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8639
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8640
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8641
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8643
Product: snapdragon_8cx_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8644
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8645
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8647
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8648
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8649
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8650
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8652
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8653
Product: snapdragon_8cx_gen_2_5g_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8654
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8656
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8657
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8658
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8659
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8660
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-SNAP-310124/8661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8662
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8663
Product: snapdragon_8cx_gen_3_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8665
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8666
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8667
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8669
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8670
Product: snapdragon_8c_compute_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8671
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8673
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8674
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8675
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8676
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8677
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8679
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8680
Product: snapdragon_8\+_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8682
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8683
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8684
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8685
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8687
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8688
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8689
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8691
Product: snapdragon_8\+_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8692
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8693
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8695
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8696
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8697
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8699
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8700
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8701
Product: snapdragon_8_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8703
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8704
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8705
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8706
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8708
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8709
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8710
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8711
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8713
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8714
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8715
Product: snapdragon_8_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8717
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8718
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8719
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8721
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8722
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8723
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8724
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-SNAP-310124/8725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Product: snapdragon_ar2_gen_1_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8726
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8727
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8728
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8730
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8731
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8732
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8734
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8735
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8736
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8738
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8739
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8740
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8741
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8743
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8744
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8745
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory allocation from TA region. **CVE ID : CVE-2023-33032**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8747
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8749
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8750
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message with multiple fragments. **CVE ID : CVE-2023-33113**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8752
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8753
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8755
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8756
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8757
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8758
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8760
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8761
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8763
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8765
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8766
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_CO	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8768
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8769
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8770
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8772
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8773
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8774
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8776
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8777
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8778
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_1300_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8780
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8781
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8782
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_2100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8784
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8785
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8786
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: snapdragon_wear_2500_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8788
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8789
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8790
Concurrent Execution using Shared Resource with	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
Product: snapdragon_wear_3100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8792
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8793
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8794
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
Product: snapdragon_wear_4100\+_platform_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8796
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8797
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8799
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8800
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33110		
Product: snapdragon_x12_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8802
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8803
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8804
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8805
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8807
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8808
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8809
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8811
Product: snapdragon_x20_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8812
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consecutively in ADSP. **CVE ID : CVE-2023-33120**		
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8814
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8815
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8816
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8818
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8819
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8820
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8821
Concurrent Execution using Shared Resource with	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8823
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8824
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8825
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8827
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8828
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8829
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8831
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8832
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8833
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8835
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8836
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8837
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8838
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8840
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8841
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8842
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8844
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8845
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8846
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8848
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8849
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8850
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verifying with RPMB data. **CVE ID : CVE-2023-33037**	ns/january-2024-bulletin	
Product: snapdragon_x5_lte_modem_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8852
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8853
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8854
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8856
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8857
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8858
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			playback with speaker protection. **CVE ID : CVE-2023-33033**	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8860
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8861
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8862
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8863
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8865
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8866
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8867
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8868
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8870
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8871
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8872
Product: snapdragon_x70_modem-rf_system_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8873
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8874
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8875
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8876
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8877
Concurrent Execution using Shared	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	security/bulletins/january-2024-bulletin	
Product: snapdragon_x75_5g_modem-rf_system_firmware					
Affected Version(s): -					
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8879
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8881
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8882
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8883
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8884
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8886
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8887
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8888
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8889
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-SNAP-310124/8890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8891
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8892
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8894
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8895
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8896
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8898
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8899
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8900
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8901
Loop with Unreachabl	02-Jan-2024	7.5	Transient DOS while parsing IPv6	https://www.qualcomm.com/c	O-QUA-SNAP-310124/8902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8903
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8904
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SNAP-310124/8905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8906
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8907
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8908
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8910
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8911
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8912
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8913
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-	O-QUA-SNAP-310124/8914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	security/bulleti ns/january-2024-bulletin	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8915
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8916
NULL Pointer Dereferenc e	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-SNAP-310124/8917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SNAP-310124/8918
Product: ssg2115p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8919
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8920
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8921
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109		
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8923
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8924
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8925
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-SSG2-310124/8926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8927
Product: ssg2125p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8928
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8929
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8931
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8932
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8933
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8935
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SSG2-310124/8936
Product: sw5100p_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8937
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SW51-310124/8938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8940
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8941
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8942
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host	https://www.qualcomm.com/company/product-	O-QUA-SW51-310124/8943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8944
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8945
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33118		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8947
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8948
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8949
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8950
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SW51-310124/8951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8952
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8953
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sw5100_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8955
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8956
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8958
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization	https://www.qualcomm.com/company/product-	O-QUA-SW51-310124/8959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with KASAN enabled. **CVE ID : CVE-2023-33094**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8960
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8961
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8962
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SW51-310124/8963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8964
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8965
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8966
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/c	O-QUA-SW51-310124/8967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	ompany/product-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8968
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8969
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8970
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SW51-310124/8971
Concurrent Execution	02-Jan-2024	7	The session index variable in PCM	https://www.qualcomm.com/c	O-QUA-SW51-310124/8972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ompany/product-security/bulletins/january-2024-bulletin	
Product: sxr1120_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8973
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8974
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8976
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8977
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8978
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: sxr1230p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8980
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8981
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8982
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8983
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response"	https://www.qualcomm.com/company/product-	O-QUA-SXR1-310124/8984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8985
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8986
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR1-310124/8988
Product: sxr2130_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8989
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8990
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8991
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8993
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8994
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8995
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SXR2-310124/8996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8997
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8998
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/8999
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9001
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9002
Product: sxr2230p_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9003
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9005
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9006
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9007
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9008
Concurrent Execution using Shared Resource with Improper Synchroniz	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9010
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-SXR2-310124/9011
Product: vision_intelligence_100_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9012
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-VISI-310124/9013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9014
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9015
Product: vision_intelligence_200_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9017
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9018
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9019
Product: vision_intelligence_300_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case.	https://www.qualcomm.com/company/product-	O-QUA-VISI-310124/9020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33030	security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9021
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9022
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9023
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9024
Concurrent Execution using Shared Resource	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-VISI-310124/9025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9026
Product: vision_intelligence_400_platform_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9027
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9028
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map	https://www.qualcomm.com/company/product-	O-QUA-VISI-310124/9029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9030
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9031
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9032
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-VISI-310124/9034
Product: wcd9306_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9035
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9036
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9038
Product: wcd9326_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9039
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9040
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33038		
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9042
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9043
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9044
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9046
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9047
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9048
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9049
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-WCD9-310124/9050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9051
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9052
Product: wcd9330_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9054
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9055
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9056
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcd9335_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9058
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9059
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9060
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9061
Buffer Copy	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	O-QUA-WCD9-310124/9062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			wearables while processing data from AON. **CVE ID : CVE-2023-33085**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9063
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9064
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9065
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9067
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9068
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9069
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33062	ns/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9071
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9072
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9073
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcd9340_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9075
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9076
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9077
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9078
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-WCD9-310124/9079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9080
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9081
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9083
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9084
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9085
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9086
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9088
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9089
Product: wcd9341_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9091
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9092
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9093
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9095
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-WCD9-310124/9096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	ompany/product-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9097
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9098
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9100
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9101
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9102
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9103
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9105
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9106
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9107
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM	https://www.qualcomm.com/company/produc	O-QUA-WCD9-310124/9108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	t-security/bulleti ns/january-2024-bulletin	
Product: wcd9360_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-WCD9-310124/9109
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-WCD9-310124/9110
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-WCD9-310124/9111
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.q ualcomm.com/c ompany/produc t-security/bulleti ns/january-2024-bulletin	O-QUA-WCD9-310124/9112
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.q ualcomm.com/c ompany/produc	O-QUA-WCD9-310124/9113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9114
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9115
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9116
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9118
Product: wcd9370_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9119
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9120
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33032	ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9122
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9123
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9124
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9125
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9127
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9128
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9129
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when	https://www.qualcomm.com/company/produc	O-QUA-WCD9-310124/9130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9131
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9132
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9133
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9134
N/A	02-Jan-2024	7.5	Transient DOS when WLAN	https://www.qualcomm.com/c	O-QUA-WCD9-310124/9135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	ompany/product-security/bulletins/january-2024-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9136
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9137
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33036		
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9139
Product: wcd9371_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9140
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9141
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9142
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9144
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9145
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9146
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9147
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9149
Product: wcd9375_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9150
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ns/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9152
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9153
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9154
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9155
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9157
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9158
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9159
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9161
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9162
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9163
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9165
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9166
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9167
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9169
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9170
Product: wcd9380_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9171
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9173
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9174
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9176
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9178
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9179
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9180
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter from ST HAL. **CVE ID : CVE-2023-33118**		
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9182
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9183
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9184
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9185
NULL Pointer	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen	https://www.qualcomm.com/company/produc	O-QUA-WCD9-310124/9186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9187
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9188
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9189
Concurrent Execution using Shared Resource with Improper Synchronization	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9191
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9192
Product: wcd9385_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9193
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9196
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9197
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9198
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9200
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9201
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9203
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9204
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9205
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9206
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33112		
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9208
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9209
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9210
NULL Pointer	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI	https://www.qualcomm.com/company/product-	O-QUA-WCD9-310124/9211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			support makes a PSCI call. **CVE ID : CVE-2023-33036**	security/bulletins/january-2024-bulletin	
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9212
Product: wcd9390_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9213
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9214
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33113		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9216
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9217
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9218
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9220
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9221
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9222
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9223
Product: wcd9395_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9224
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9225
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9226
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9227
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client	https://www.qualcomm.com/company/product-	O-QUA-WCD9-310124/9228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9229
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9230
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9231
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-310124/9232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33109	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9233
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCD9-310124/9234
Product: wcn3610_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9235
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9237
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9238
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9239
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9241
Product: wcn3615_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9242
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9243
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33094		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9245
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9246
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9247
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9249
Product: wcn3620_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9250
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9251
Use After Free	02-Jan-2024	7.8	Memory corruption in	https://www.qualcomm.com/c	O-QUA-WCN3-310124/9252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	ompany/product-security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9253
Product: wcn3660b_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9255
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9257
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9258
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9260
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9261
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9262
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	ns/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9264
Product: wcn3660_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9265
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9266
Concurrent Execution	02-Jan-2024	7	The session index variable in PCM	https://www.qualcomm.com/c	O-QUA-WCN3-310124/9267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	ompany/product-security/bulletins/january-2024-bulletin	
Product: wcn3680b_firmware					
Affected Version(s): -					
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9268
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9269
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33033	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9271
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9272
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9273
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9275
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9276
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn3680_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9278
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9279
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9280
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcn3910_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9282
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9283
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9284
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9286
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9287
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9288
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33040	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9290
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9291
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9292
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing memory corruption. **CVE ID : CVE-2023-33110**		
Product: wcn3950_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9294
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9295
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9296
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9297
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-	O-QUA-WCN3-310124/9298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	security/bulletins/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9299
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9300
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9301
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9303
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9304
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9305
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9307
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9308
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9309
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9310
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9312
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9313
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9314
Product: wcn3980_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9315
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9316
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9317
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9318
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9320
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9321
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9322
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9323
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the	https://www.qualcomm.com/company/produc	O-QUA-WCN3-310124/9324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9325
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9326
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9328
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9329
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9330
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9331
Out-of-bounds Read	02-Jan-2024	7.5	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver. **CVE ID : CVE-2023-33116**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9332
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-WCN3-310124/9333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9334
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9335
Product: wcn3988_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33025**	ns/january-2024-bulletin	
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9337
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9338
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9339
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9340
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket Transport Server. **CVE ID : CVE-2023-33038**	ns/january-2024-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9342
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9343
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9344
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9346
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9347
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9348
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-310124/9349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9350
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9351
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9352
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9353
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9355
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9356
Product: wcn3990_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9358
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9359
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9360
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9361
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9363
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9364
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9365
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-WCN3-310124/9366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9367
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9368
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9369
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback -	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9371
Product: wcn3999_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9372
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9373
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9374
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware	https://www.qualcomm.com/c	O-QUA-WCN3-310124/9375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while parsing a BTM request. **CVE ID : CVE-2023-33062**	ompany/product-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9376
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9377
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN3-310124/9378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn6740_firmware					
Affected Version(s): -					
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9379
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9380
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9382
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9384
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9385
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9386
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33120		
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9388
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9389
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9390
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9391
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43511		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WCN6-310124/9393
Product: wsa8810_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9394
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28583		
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9396
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9397
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9398
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9401
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9402
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9403
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9405
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9406
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9407
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9409
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9410
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9411
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9412
Concurrent Execution using Shared Resource with Improper Synchroniz	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**		
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9414
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9415
Product: wsa8815_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9416
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9418
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region. **CVE ID : CVE-2023-33032**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9419
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9420
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9421
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9423
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9424
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time. **CVE ID : CVE-2023-33114**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9425
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-310124/9426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9427
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9428
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9429
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during DTLS handshake. **CVE ID : CVE-2023-33040**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9431
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9432
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9433
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9434
Concurrent Execution using	02-Jan-2024	7	The session index variable in PCM host voice audio	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	t-security/bulletins/january-2024-bulletin	
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9436
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9437
Product: wsa8830_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2023-33025**		
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9439
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9440
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9441
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9442
Buffer Copy without Checking Size of Input	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON.	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-310124/9443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2023-33085**	ns/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9444
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9445
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9446
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33114		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9448
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9449
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9450
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-310124/9451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9452
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9453
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9454
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9455
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9457
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9458
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9459
Product: wsa8832_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call. **CVE ID : CVE-2023-33025**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9460
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9461
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9462
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9463
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9465
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9466
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9467
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9468
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9470
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9471
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data. **CVE ID : CVE-2023-33037**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9472
Product: wsa8835_firmware					
Affected Version(s): -					
Buffer Copy without Checking	02-Jan-2024	9.8	Memory corruption in Data Modem when a non-standard SDP	https://www.qualcomm.com/company/product-	O-QUA-WSA8-310124/9473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			body, during a VOLTE call. **CVE ID : CVE-2023-33025**	security/bulletins/january-2024-bulletin	
Double Free	02-Jan-2024	7.8	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address. **CVE ID : CVE-2023-28583**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9474
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in HLOS while running playready use-case. **CVE ID : CVE-2023-33030**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9475
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption in Audio during playback with speaker protection. **CVE ID : CVE-2023-33033**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9476
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption while receiving a message in Bus Socket Transport Server. **CVE ID : CVE-2023-33038**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9477
Buffer Copy without	02-Jan-2024	7.8	Memory corruption in wearables while	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			processing data from AON. **CVE ID : CVE-2023-33085**	t-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9479
Use After Free	02-Jan-2024	7.8	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued. **CVE ID : CVE-2023-33108**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9480
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9481
Use After Free	02-Jan-2024	7.8	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are submitted at the same time. **CVE ID : CVE-2023-33114**		
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9483
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9484
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9485
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	t-security/bulletins/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in Data Modem during DTLS handshake. **CVE ID : CVE-2023-33040**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9487
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9488
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9489
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9490
Loop with Unreachable Exit Condition	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN	https://www.qualcomm.com/company/product-	O-QUA-WSA8-310124/9491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	security/bulletins/january-2024-bulletin	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Jan-2024	7	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption. **CVE ID : CVE-2023-33110**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9492
NULL Pointer Dereference	02-Jan-2024	5.5	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call. **CVE ID : CVE-2023-33036**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9493
Missing Encryption of Sensitive Data	02-Jan-2024	5.5	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33037		
Product: wsa8840_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9495
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9496
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9497
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33117		
Use After Free	02-Jan-2024	7.8	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9499
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9500
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9501
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9503
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9504
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9505
Product: wsa8845h_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9506
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK	https://www.qualcomm.com/company/produc	O-QUA-WSA8-310124/9507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	t-security/bulletins/january-2024-bulletin	
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9508
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9509
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9510
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-310124/9511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9512
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host. **CVE ID : CVE-2023-33109**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9513
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9514
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9515
Product: wsa8845_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Jan-2024	7.8	Memory corruption in wearables while processing data from AON. **CVE ID : CVE-2023-33085**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9516
Use After Free	02-Jan-2024	7.8	Memory corruption while running VK synchronization with KASAN enabled. **CVE ID : CVE-2023-33094**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9517
Out-of-bounds Write	02-Jan-2024	7.8	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments. **CVE ID : CVE-2023-33113**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9518
Use After Free	02-Jan-2024	7.8	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command. **CVE ID : CVE-2023-33117**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9519
Use After Free	02-Jan-2024	7.8	Memory corruption while	https://www.qualcomm.com/c	O-QUA-WSA8-310124/9520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL. **CVE ID : CVE-2023-33118**	ompany/product-security/bulletins/january-2024-bulletin	
Use After Free	02-Jan-2024	7.8	Memory corruption in Audio when memory map command is executed consecutively in ADSP. **CVE ID : CVE-2023-33120**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9521
Use After Free	02-Jan-2024	7.8	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP. **CVE ID : CVE-2023-43514**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9522
N/A	02-Jan-2024	7.5	Transient DOS in WLAN Firmware while parsing a BTM request. **CVE ID : CVE-2023-33062**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9523
NULL Pointer Dereference	02-Jan-2024	7.5	Transient DOS while processing a WMI P2P listen start command	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-310124/9524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0xD00A) sent from host. **CVE ID : CVE-2023-33109**	ns/january-2024-bulletin	
N/A	02-Jan-2024	7.5	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element. **CVE ID : CVE-2023-33112**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9525
Loop with Unreachable Exit Condition ('Infinite Loop')	02-Jan-2024	7.5	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header. **CVE ID : CVE-2023-43511**	https://www.qualcomm.com/company/product-security/bulletins/january-2024-bulletin	O-QUA-WSA8-310124/9526
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	7.8	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through	https://access.redhat.com/security/cve/CVE-2023-6004, https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LZQVUHWVWRH73YBXUQJOD6CKHDQBU3DM/	O-RED-ENTE-310124/9527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the hostname parameter. **CVE ID : CVE-2023-6004**		
Out-of-bounds Read	08-Jan-2024	7.8	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. **CVE ID : CVE-2021-3600**	https://git.kernel.org/linus/e88b2c6e5a4d9ce30d75391e4d950da74bb2bd90	O-RED-ENTE-310124/9528
Out-of-bounds Write	02-Jan-2024	5.3	A stack based buffer overflow was found in the virtio-net device of QEMU. This issue occurs when flushing TX in the virtio_net_flush_tx function if guest features VIRTIO_NET_F_HASH_REPORT, VIRTIO_F_VERSION_1 and VIRTIO_NET_F_MRG_RXBUF are enabled. This could allow a malicious user to overwrite local variables allocated on the stack. Specifically, the `out_sg`	https://bugzilla.redhat.com/show_bug.cgi?id=2254580	O-RED-ENTE-310124/9529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable could be used to read a part of process memory and send it to the wire, causing an information leak. **CVE ID : CVE-2023-6693**		
Missing Release of Memory after Effective Lifetime	02-Jan-2024	4.4	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow. **CVE ID : CVE-2023-7192**	https://bugzilla.redhat.com/show_bug.cgi?id=2256279, https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=ac4893980bbe79ce383daf9a0885666a30fe4c83	O-RED-ENTE-310124/9530
Use After Free	03-Jan-2024	3.3	A use-after-free flaw was found in PackageKitd. In some conditions, the order of cleanup mechanics for a transaction could be impacted. As a result, some memory access could occur on memory regions that were previously freed. Once freed, a memory region can	https://bugzilla.redhat.com/show_bug.cgi?id=2256624	O-RED-ENTE-310124/9531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be reused for other allocations and any previously stored data in this memory region is considered lost. **CVE ID : CVE-2024-0217**		
Affected Version(s): 9.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Jan-2024	7.8	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter. **CVE ID : CVE-2023-6004**	https://access.redhat.com/security/cve/CVE-2023-6004, https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/LZQVUHWVWRH73YBXUQJOD6CKHDQBU3DM/	O-RED-ENTE-310124/9532
Use After Free	02-Jan-2024	6.7	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-collected when the pipapo set is removed, the element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN	https://bugzilla.redhat.com/show_bug.cgi?id=2255653	O-RED-ENTE-310124/9533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object or NFT_OBJECT object, allowing a local unprivileged user with CAP_NET_ADMIN capability to escalate their privileges on the system. **CVE ID : CVE-2024-0193**		
Out-of-bounds Write	02-Jan-2024	5.3	A stack based buffer overflow was found in the virtio-net device of QEMU. This issue occurs when flushing TX in the virtio_net_flush_tx function if guest features VIRTIO_NET_F_HASH_REPORT, VIRTIO_F_VERSION_1 and VIRTIO_NET_F_MRG_RXBUF are enabled. This could allow a malicious user to overwrite local variables allocated on the stack. Specifically, the `out_sg` variable could be used to read a part of process memory and send it to the wire, causing an information leak. **CVE ID : CVE-2023-6693**	https://bugzilla.redhat.com/show_bug.cgi?id=2254580	O-RED-ENTE-310124/9534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-Jan-2024	4.4	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow. **CVE ID : CVE-2023-7192**	https://bugzilla.redhat.com/show_bug.cgi?id=2256279, https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=ac4893980bbe79ce383daf9a0885666a30fe4c83	O-RED-ENTE-310124/9535
Use After Free	03-Jan-2024	3.3	A use-after-free flaw was found in PackageKitd. In some conditions, the order of cleanup mechanics for a transaction could be impacted. As a result, some memory access could occur on memory regions that were previously freed. Once freed, a memory region can be reused for other allocations and any previously stored data in this memory region is considered lost. **CVE ID : CVE-2024-0217**	https://bugzilla.redhat.com/show_bug.cgi?id=2256624	O-RED-ENTE-310124/9536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Samsung					
Product: android					
Affected Version(s): 11.0					
Improper Authentication	04-Jan-2024	6.5	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction. **CVE ID : CVE-2024-20803**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9537
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2024-20804**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9538
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to write arbitrary file. **CVE ID : CVE-2024-20805**		
N/A	04-Jan-2024	5.5	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data. **CVE ID : CVE-2024-20806**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9540
Affected Version(s): 12.0					
Improper Authentication	04-Jan-2024	6.5	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction. **CVE ID : CVE-2024-20803**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9541
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file.	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20804		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2024-20805**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9543
N/A	04-Jan-2024	5.5	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data. **CVE ID : CVE-2024-20806**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9544
Affected Version(s): 13.0					
Improper Authentication	04-Jan-2024	6.5	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction. **CVE ID : CVE-2024-20803**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2024-20804**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9546
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jan-2024	5.5	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file. **CVE ID : CVE-2024-20805**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9547
N/A	04-Jan-2024	5.5	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data. **CVE ID : CVE-2024-20806**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9548
Affected Version(s): 14.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Jan-2024	6.5	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction. **CVE ID : CVE-2024-20803**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9549
N/A	04-Jan-2024	5.5	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data. **CVE ID : CVE-2024-20806**	https://security.samsungmobile.com/securityUpdate.smsb?year=2024&month=01	O-SAM-ANDR-310124/9550
Vendor: Tenda					
Product: a18_firmware					
Affected Version(s): 15.13.07.09					
Out-of-bounds Write	09-Jan-2024	9.8	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2023-50585**	N/A	O-TEN-A18_-310124/9551
Product: ax12_firmware					
Affected Version(s): 22.03.01.46					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Jan-2024	7.5	Buffer Overflow vulnerability in Tenda AX12 V22.03.01.46, allows remote attackers to cause a denial of service (DoS) via list parameter in SetNetControlList function. **CVE ID : CVE-2023-49427**	N/A	O-TEN-AX12-310124/9552
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function getIptvInfo. **CVE ID : CVE-2023-51971**	N/A	O-TEN-AX18-310124/9553
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 was discovered to contain a command injection vulnerability via the function fromAdvSetLanIp. **CVE ID : CVE-2023-51972**	N/A	O-TEN-AX18-310124/9554
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the	N/A	O-TEN-AX18-310124/9555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function formGetIptv. **CVE ID : CVE-2023-51961**		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo. **CVE ID : CVE-2023-51966**	N/A	O-TEN-AX18-310124/9556
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formSetIptv. **CVE ID : CVE-2023-51952**	N/A	O-TEN-AX18-310124/9557
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv. **CVE ID : CVE-2023-51953**	N/A	O-TEN-AX18-310124/9558
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formSetIptv.	N/A	O-TEN-AX18-310124/9559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51954		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formSetIptv. **CVE ID : CVE-2023-51955**	N/A	O-TEN-AX18-310124/9560
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formSetIptv **CVE ID : CVE-2023-51956**	N/A	O-TEN-AX18-310124/9561
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv. **CVE ID : CVE-2023-51957**	N/A	O-TEN-AX18-310124/9562
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv. **CVE ID : CVE-2023-51958**	N/A	O-TEN-AX18-310124/9563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv. **CVE ID : CVE-2023-51959**	N/A	O-TEN-AX18-310124/9564
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv. **CVE ID : CVE-2023-51960**	N/A	O-TEN-AX18-310124/9565
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo. **CVE ID : CVE-2023-51963**	N/A	O-TEN-AX18-310124/9566
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo. **CVE ID : CVE-2023-51964**	N/A	O-TEN-AX18-310124/9567
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the	N/A	O-TEN-AX18-310124/9568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adv.iptv.stbpvid parameter in the function setIptvInfo. **CVE ID : CVE-2023-51965**		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo. **CVE ID : CVE-2023-51962**	N/A	O-TEN-AX18-310124/9569
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function getIptvInfo. **CVE ID : CVE-2023-51967**	N/A	O-TEN-AX18-310124/9570
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function getIptvInfo. **CVE ID : CVE-2023-51968**	N/A	O-TEN-AX18-310124/9571
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function getIptvInfo.	N/A	O-TEN-AX18-310124/9572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51969		
Out-of-bounds Write	10-Jan-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formSetIptv. **CVE ID : CVE-2023-51970**	N/A	O-TEN-AX18-310124/9573
Product: ax3_firmware					
Affected Version(s): 16.03.12.11					
N/A	04-Jan-2024	9.8	Tenda AX3 v16.03.12.11 was discovered to contain a remote code execution (RCE) vulnerability via the list parameter at /goform/SetNetControlList. **CVE ID : CVE-2023-51812**	N/A	O-TEN-AX3_-310124/9574
Product: i29_firmware					
Affected Version(s): 1.0.0.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.5	Buffer Overflow vulnerability in Tenda i29 versions 1.0 V1.0.0.5 and 1.0 V1.0.0.2, allows remote attackers to cause a denial of service (DoS) via the pingIp parameter in the pingSet function. **CVE ID : CVE-2023-50991**	N/A	O-TEN-I29_-310124/9575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.0.5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Jan-2024	7.5	Buffer Overflow vulnerability in Tenda i29 versions 1.0 V1.0.0.5 and 1.0 V1.0.0.2, allows remote attackers to cause a denial of service (DoS) via the pingIp parameter in the pingSet function. **CVE ID : CVE-2023-50991**	N/A	O-TEN-I29_-310124/9576
Vendor: totolink					
Product: lr1200gb_firmware					
Affected Version(s): 9.1.0u.6619_b20230130					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249858 is the identifier assigned to this	N/A	O-TOT-LR12-310124/9577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0292**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this vulnerability is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249859. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TOT-LR12-310124/9578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0293		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this issue is the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249860. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0294**	N/A	O-TOT-LR12-310124/9579
Improper Neutralization of Special Elements used in an OS	08-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B2023	N/A	O-TOT-LR12-310124/9580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			0130. This affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249861 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0295**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Jan-2024	8.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to command	N/A	O-TOT-LR12-310124/9581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249857 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0291**		
Product: n200re_firmware					
Affected Version(s): 9.3.5u.6139_b20201216					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-	N/A	O-TOT-N200-310124/9582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			249862 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-2024-0296**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249863. NOTE: The vendor was contacted early about this disclosure but did	N/A	O-TOT-N200-310124/9583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0297**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. Affected is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command 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-249864. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0298**	N/A	O-TOT-N200-310124/9584
Improper Neutralization of Special Elements used in an OS	08-Jan-2024	9.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. Affected by this	N/A	O-TOT-N200-310124/9585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249865 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0299**		
Product: n350rt_firmware					
Affected Version(s): 9.3.5u.6139_b20201216					
Stack-based Buffer Overflow	09-Jan-2024	9.8	A vulnerability has been found in Totolink N350RT 9.3.5u.6139_B202012 and classified as critical. Affected by this vulnerability is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host	N/A	O-TOT-N350-310124/9586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7219**		
Out-of-bounds Write	07-Jan-2024	8.8	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this vulnerability is the function main of the file /cgi-bin/cstecgi.cgi?action=login&flag=1 of the component HTTP POST Request Handler. The manipulation of the argument v33 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has	N/A	O-TOT-N350-310124/9587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier VDB-249769 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7213**		
Out-of-bounds Write	07-Jan-2024	8.8	A vulnerability, which was classified as critical, has been found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this issue is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v8 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249770 is the identifier assigned	N/A	O-TOT-N350-310124/9588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7214**		
Stack-based Buffer Overflow	08-Jan-2024	7.2	A vulnerability, which was classified as critical, was found in Totolink N350RT 9.3.5u.6139_B202012. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-249852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7218**	N/A	O-TOT-N350-310124/9589
Product: nr1800x_firmware					
Affected Version(s): 9.1.0u.6279_b20210910					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	09-Jan-2024	9.8	A vulnerability was found in Totolink NR1800X 9.1.0u.6279_B20210910 and classified as critical. Affected by this issue is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249854 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-2023-7220**	N/A	O-TOT-NR18-310124/9590
Product: t6_firmware					
Affected Version(s): 4.1.9cu.5241_b20210923					
Buffer Copy without Checking Size of Input ('Classic	09-Jan-2024	9.8	A vulnerability was found in Totolink T6 4.1.9cu.5241_B20210923. It has been classified as critical. This affects the function main	N/A	O-TOT-T6_F-310124/9591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v41 leads to buffer overflow. 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-249855. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7221**		
Improper Access Control	09-Jan-2024	6.5	A vulnerability classified as problematic has been found in Totolink T6 4.1.9cu.5241_B20210923. This affects an unknown part of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument topicurl with the input showSyslog leads	N/A	O-TOT-T6_F-310124/9592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper access controls. 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-249867. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7223**		
Product: x2000r_firmware					
Affected Version(s): 1.0.0-b20221212.1452					
Out-of-bounds Write	09-Jan-2024	9.8	A vulnerability was found in Totolink X2000R 1.0.0-B20221212.1452. It has been declared as critical. This vulnerability affects the function formTmultiAP of the file /bin/boa of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack can be initiated remotely. The exploit has	N/A	O-TOT-X200-310124/9593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249856. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7222**		
Affected Version(s): 2.0.0-b20230727.10434					
Out-of-bounds Write	07-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink X2000R_V2 2.0.0-B20230727.10434. This vulnerability affects the function formTmultiAP of the file /bin/boa. The manipulation leads to buffer overflow. VDB-249742 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-2023-7208**	N/A	O-TOT-X200-310124/9594
Vendor: Trendnet					
Product: tv-ip1314pi_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.5.3					
N/A	09-Jan-2024	9.8	An issue was discovered in libremote_dbg.so on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Filtering of debug information is mishandled during use of popen. Consequently, an attacker can bypass validation and execute a shell command. **CVE ID : CVE-2023-49235**	https://drive.google.com/file/d/1lTloBkH_7zAz1ZbFVSZnfpoPd81aPaHx/view?usp=sharing	O-TRE-TV-I-310124/9595
Out-of-bounds Write	09-Jan-2024	9.8	A stack-based buffer overflow was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices, leading to arbitrary command execution. This occurs because of lack of length validation during an sscanf of a user-entered scale field in the RTSP playback function of davinci. **CVE ID : CVE-2023-49236**	https://drive.google.com/file/d/1lTloBkH_7zAz1ZbFVSZnfpoPd81aPaHx/view?usp=sharing	O-TRE-TV-I-310124/9596
Vendor: uniwayinfo					
Product: uw-101x_firmware					
Affected Version(s): * Up to (including) 2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**	N/A	O-UNI-UW-1-310124/9597
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by	N/A	O-UNI-UW-1-310124/9598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**		
Product: uw-301vpw_firmware					
Affected Version(s): * Up to (including) 2.0					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip	N/A	O-UNI-UW-3-310124/9599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has	N/A	O-UNI-UW-3-310124/9600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. VDB-249758 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-2023-7209**		
Product: uw-302vp_firmware					
Affected Version(s): * Up to (including) 2.0					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be	N/A	O-UNI-UW-3-310124/9601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-249766 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-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-UNI-UW-3-310124/9602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-7209		
Product: uw-311vpw_firmware					
Affected Version(s): * Up to (including) 2.0					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**	N/A	O-UNI-UW-3-310124/9603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**	N/A	O-UNI-UW-3-310124/9604
Product: uw-323dac_firmware					
Affected Version(s): * Up to (including) 2.0					
Improper Authentication	07-Jan-2024	8.1	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the	N/A	O-UNI-UW-3-310124/9605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 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-2023-7211**		
Improper Resource Shutdown or Release	07-Jan-2024	7.5	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The	N/A	O-UNI-UW-3-310124/9606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 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-2023-7209**		
Vendor: XEN					
Product: xen					
Affected Version(s): -					
Uncontrolled Resource Consumption	05-Jan-2024	4.9	Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is	https://xenbits.xenproject.org/xsa/advisory-441.html	O-XEN-XEN-310124/9607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock). **CVE ID : CVE-2023-34324**		
Affected Version(s): *					
Out-of-bounds Write	05-Jan-2024	7.8	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.]	https://xenbits.xenproject.org/xsa/advisory-443.html	O-XEN-XEN-310124/9608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libfsimage contains parsing code for several filesystems, most of them based on grub-legacy code. libfsimage is used by pygrub to inspect guest disks. Pygrub runs as the same user as the toolstack (root in a priviledged domain). At least one issue has been reported to the Xen Security Team that allows an attacker to trigger a stack buffer overflow in libfsimage. After further analisys the Xen Security Team is no longer confident in the suitability of libfsimage when run against guest controlled input with super user priviledges. In order to not affect current deployments that rely on pygrub patches are provided in the resolution section of the advisory that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow running pygrub in deprivileged mode. CVE-2023-4949 refers to the original issue in the upstream grub project ("An attacker with local access to a system (either through a disk or external drive) can present a modified XFS partition to grub-legacy in such a way to exploit a memory corruption in grub's XFS file system implementation.") CVE-2023-34325 refers specifically to the vulnerabilities in Xen's copy of libfsimage, which is decended from a very old version of grub. **CVE ID : CVE-2023-34325**		
N/A	05-Jan-2024	7.8	The caching invalidation guidelines from the AMD-Vi specification (48882—Rev	https://xenbits.xenproject.org/xsa/advisory-442.html	O-XEN-XEN-310124/9609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.07-PUB—Oct 2022) is incorrect on some hardware, as devices will malfunction (see stale DMA mappings) if some fields of the DTE are updated but the IOMMU TLB is not flushed. Such stale DMA mappings can point to memory ranges not owned by the guest, thus allowing access to unindented memory regions. **CVE ID : CVE-2023-34326**		
N/A	05-Jan-2024	5.5	The current setup of the quarantine page tables assumes that the quarantine domain (dom_io) has been initialized with an address width of DEFAULT_DOMAIN_ADDRESS_WIDTH (48) and hence 4 page table levels. However dom_io being a PV domain gets the AMD-Vi IOMMU page tables levels based on the maximum (hot pluggable) RAM	https://xenbits.xenproject.org/xsa/advisory-445.html	O-XEN-XEN-310124/9610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address, and hence on systems with no RAM above the 512GB mark only 3 page-table levels are configured in the IOMMU. On systems without RAM above the 512GB boundary amd_iommu_quarantine_init() will setup page tables for the scratch page with 4 levels, while the IOMMU will be configured to use 3 levels only, resulting in the last page table directory (PDE) effectively becoming a page table entry (PTE), and hence a device in quarantine mode gaining write access to the page destined to be a PDE. Due to this page table level mismatch, the sink page the device gets read/write access to is no longer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleared between device assignment, possibly leading to data leaks. **CVE ID : CVE-2023-46835**		
N/A	05-Jan-2024	4.7	The fixes for XSA-422 (Branch Type Confusion) and XSA-434 (Speculative Return Stack Overflow) are not IRQ-safe. It was believed that the mitigations always operated in contexts with IRQs disabled. However, the original XSA-254 fix for Meltdown (XPTI) deliberately left interrupts enabled on two entry paths; one unconditionally, and one conditionally on whether XPTI was active. As BTC/SRSO and Meltdown affect different CPU vendors, the mitigations are not active together by default.	https://xenbits.xenproject.org/xsa/advisory-446.html	O-XEN-XEN-310124/9611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Therefore, there is a race condition whereby a malicious PV guest can bypass BTC/SRSO protections and launch a BTC/SRSO attack against Xen. **CVE ID : CVE-2023-46836**		
Affected Version(s): * Up to (excluding) 4.17.0					
NULL Pointer Dereference	05-Jan-2024	5.5	When a transaction is committed, C Xenstored will first check the quota is correct before attempting to commit any nodes. It would be possible that accounting is temporarily negative if a node has been removed outside of the transaction. Unfortunately, some versions of C Xenstored are assuming that the quota cannot be negative and are using assert() to confirm it. This will lead to C Xenstored crash when tools are	https://xenbits.xenproject.org/xsa/advisory-440.html	O-XEN-XEN-310124/9612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			built without -DNDEBUG (this is the default). **CVE ID : CVE-2023-34323**		
Affected Version(s): * Up to (including) 4.16					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jan-2024	3.3	Arm provides multiple helpers to clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory. **CVE ID : CVE-2023-34321**	https://xenbits.xenproject.org/xsa/advisory-437.html	O-XEN-XEN-310124/9613
Improper Restriction	05-Jan-2024	3.3	Arm provides multiple helpers to	https://xenbits.xenproject.org/	O-XEN-XEN-310124/9614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory. This undefined behavior was meant to be addressed by XSA-437, but the approach was not sufficient. **CVE ID : CVE-2023-46837**	xsa/advisory-447.html	
Affected Version(s): From (including) 3.2.0 Up to (excluding) 4.15.0					
Improper Check for	05-Jan-2024	7.8	For migration as well as to work	https://xenbits.xenproject.org/	O-XEN-XEN-310124/9615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dropped Privileges			around kernels unaware of L1TF (see XSA-273), PV guests may be run in shadow paging mode. Since Xen itself needs to be mapped when PV guests run, Xen and shadowed PV guests run directly the respective shadow page tables. For 64-bit PV guests this means running on the shadow of the guest root page table. In the course of dealing with shortage of memory in the shadow pool associated with a domain, shadows of page tables may be torn down. This tearing down may include the shadow root page table that the CPU in question is presently running on. While a precaution exists to	xsa/advisory-438.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supposedly prevent the tearing down of the underlying live page table, the time window covered by that precaution isn't large enough. **CVE ID : CVE-2023-34322**		
Affected Version(s): From (including) 4.5.0 Up to (excluding) 4.14.0					
N/A	05-Jan-2024	5.5	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] AMD CPUs since ~2014 have extensions to normal x86 debugging functionality. Xen supports guests using these extensions. Unfortunately there are errors in Xen's handling of the guest state, leading to denials of service. 1) CVE-2023-34327 - An HVM	https://xenbits.xenproject.org/xsa/advisory-444.html	O-XEN-XEN-310124/9616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vCPU can end up operating in the context of a previous vCPUs debug mask state. 2) CVE-2023-34328 - A PV vCPU can place a breakpoint over the live GDT. This allows the PV vCPU to exploit XSA-156 / CVE-2015-8104 and lock up the CPU entirely. **CVE ID : CVE-2023-34328**		
Vendor: ZTE					
Product: red_magic_8_pro_firmware					
Affected Version(s): gen_cn_nx729jv1.0.0b21mr					
N/A	04-Jan-2024	5.5	Permissions and Access Control Vulnerability in ZTE Red Magic 8 Pro **CVE ID : CVE-2023-41784**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034444	O-ZTE-RED_-310124/9617
Product: zxcloud_irai_firmware					
Affected Version(s): * Up to (excluding) 7.23.30					
Uncontrolled Search Path Element	05-Jan-2024	4.8	There is a DLL hijacking vulnerability in ZTE ZXCLOUD iRAI, an attacker could place a fake DLL file in a specific	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1032984	O-ZTE-ZXCL-310124/9618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory and successfully exploit this vulnerability to execute malicious code. **CVE ID : CVE-2023-41782**		
Affected Version(s): * Up to (excluding) 7.23.32					
Improper Privilege Management	03-Jan-2024	7.8	There is a local privilege escalation vulnerability of ZTE's ZXCLOUD iRAI.Attackers with regular user privileges can create a fake process, and to escalate local privileges. **CVE ID : CVE-2023-41776**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	O-ZTE-ZXCL-310124/9619
Uncontrolled Search Path Element	03-Jan-2024	7.8	There is an unsafe DLL loading vulnerability in ZTE ZXCLOUD iRAI. Due to the program failed to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges. **CVE ID : CVE-2023-41780**	https://https//support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	O-ZTE-ZXCL-310124/9620
Improper Control of Generation of Code	03-Jan-2024	7.8	There is a command injection vulnerability of ZTE's ZXCLOUD iRAI. Due to the program failed	https://support.zte.com.cn/support/news/LoopholeInfoDetail.	O-ZTE-ZXCL-310124/9621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges. **CVE ID : CVE-2023-41783**	aspx?newsId=1034404	
Incorrect Authorization	03-Jan-2024	5.5	There is an illegal memory access vulnerability of ZTE's ZXCLOUD iRAI product.When the vulnerability is exploited by an attacker with the common user permission, the physical machine will be crashed. **CVE ID : CVE-2023-41779**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1034404	O-ZTE-ZXCL-310124/9622